IRS

FATCA | Foreign Account Tax Compliance Act

International Data Exchange Services (IDES)

User Guide

Publication 5190 (01-2015) Catalog Number 67386F Department of the Treasury Internal Revenue Service IRS.gov

Table of Contents

TABLE OF CONTENTS **2**

DISCLAIMERS **5**

1. INTRODUCTION **6**

About FATCA 6

Purpose of Guide 6

Comments 7

Technical Support 7

2. INTERNATIONAL DATA EXCHANGE SERVICE (IDES) **7**

About IDES 7

Before You Begin 8

Authorized Users 8

System Availability 10

Data Security 10

File Retention 11

Requirements 11

HCTA Username and Password 12

3. OBTAINING A DIGITAL CERTIFICATE **12**

Purpose of a Digital Certificate 12

IRS Approved Certificate Authorities 12

Upload a Digital Certificate to IDES 13

Public Key Certificate 13

Certificate Maintenance 13

4. IDES ENROLLMENT **13**

Overview 14

Accessing the IDES Enrollment Site 14

IDES Enrollment Home Page 14

Enrollment Tab 16

Knowledge Base Tab 16

Support Tab 18

IRS Public Key Tab 19

IDES Enrollment User Log In Tab 19

5. HCTA ADMINISTRATORS **21**

DRAFT

Overview 21
Begin Enrollment 22
Create Challenge Questions 25
Create User Profile 26
Select Alert Preferences 27
Upload Digital Certificate 28

6. FI ADMINISTRATORS 30

Overview 30
Begin Enrollment 31
Create Challenge Questions 33
Create User Profile 35
Select Alert Preferences 37
Upload Digital Certificate 38

7. EXISTING ADMINISTRATORS (HCTA AND FI) 40

Add a User 40
Disable a User 42
Enable a User 45
Update the Certificate 48
Update Alert Preferences 50
Create a Metadata File 52
Reset Password 55
Download the IRS Public Key 58

8. END USERS 59

Create an Account 59
Create Challenge Questions 60
Create User Profile 61
Select Alert Preferences 62
IDES Enrollment User Log In 64
Create a Metadata File 66
Update Alert Preferences 67
Reset Password 69
Forgot Username 70
Forgot Password 74

9. PREPARING THE FATCA XML 77

DRAFT

Preparing the FATCA XML File 77
Step 1 - Prepare and Validate the FATCA XML File 78
Step 1a - Sign the XML File 78
Step 2 - Compress the XML File 79
Step 3 - Encrypt the XML File with AES 256 Key 80
Step 4 - Encrypt the AES Key with Public Key of Recipient 80
Step 5 - Encrypt the AES Key – Model 1, Option 2 81
Step 6 - Create Sender Metadata File 82
Step 7 - Create a FATCA Data Packet 82
Step 8 - Transmit Data Packet using IDES 83
Receiving a Notification Message from IRS 83

APPENDIX A: ACRONYMS 85

APPENDIX B: FILE NAMING CONVENTION 86

APPENDIX C: CERTIFICATE UPLOAD ERROR MESSAGES 87

DRAFT

Disclaimers

IRS Disclaimer:
This document is a draft and is being provided to the public for information purposes only. Information in this document is indicative, and is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, for any purpose, without the express written of permission the IRS.

All screen shots that appear throughout the IDES User Guide (IRS Publication 5190) are used with the permission of IRS. The screen shots used in this publication—or any other screen shots from IDES or its affiliated programs—may not be extracted, copied, or distributed without written approval from the IRS SPEC Office of Products, Systems, & Analysis.

DRAFT

Unisys Disclaimer:
The software and accompanying documentation are commercial computer software and commercial computer software documentation developed at private expense. Use, reproduction, or disclosure by the Government is subject to the terms of Unisys standard commercial license for the products, and where applicable, the restricted/limited rights provisions of the contract data rights clauses.

Copyright © 2014 Unisys Corporation
All rights reserved.

An Additional Note About Screen Shots:

Screen shots contained in this draft are intended for illustrative purposes only and may not match the IDES Enrollment site exactly. The FATCA IDES team will continue to update screen shots in future versions of the guide.

1. Introduction

About FATCA

The Foreign Account Tax Compliance Act (FATCA) was enacted as part of the Hiring Incentives to Restore Employment (HIRE) Act in March 2010. FATCA was created to improve transparency and address tax non-compliance by US taxpayers. Generally, FATCA requires foreign financial institutions (FFIs) to report to the IRS certain information about financial accounts held by specified U.S. persons or by foreign entities with one or more substantial U.S. owners, or face 30 percent withholding on certain US-source payments (withholdable payments). An FFI commits to the reporting requirement by registering and signing an FFI agreement with the IRS. In addition, FATCA requires withholding agents to withhold 30 percent on withholdable payments made to passive non-financial foreign entities (NFFEs) that do not provide information on their substantial U.S. owners to withholding agents. An NFFE may elect to report directly to the IRS certain information about its substantial U.S. owners in lieu of providing such information to withholding agents (direct reporting NFFE). FATCA also requires US withholding agents to report to the IRS information about substantial US owners of a payee that is a passive NFFE and specified US persons holding certain equity or debt interests in a payee that the withholding agent has agreed to treat as an owner-documented FFI. For more information on what to report under FATCA, see the Instructions for Form 8966 (FATCA Report).

Financial Institutions (FIs) and direct reporting NFFEs that register with the IRS under FATCA are issued a Global Intermediary Identification Number (GIIN) and appear on the FFI List published by the IRS. The FFI List Search and Download tool allows users to search entities by GIIN, financial institution name, or country. For more information on FATCA, visit the FATCA Home Page.

To facilitate FATCA implementation for FIs operating in jurisdictions with laws that prevent the FIs from complying with the terms of the FFI agreement, the Treasury Department developed two alternative model intergovernmental agreements (IGAs) (Model 1 IGA and Model 2 IGA) that allow FIs operating in such jurisdictions to perform due diligence and reporting on their account holders to achieve the objectives of FATCA.

Purpose of Guide

This guide is intended to serve as a tool for FIs and Host Country Tax Authorities (HCTAs) who enroll in the International Data Exchange Service (IDES) to transmit FATCA data. The document assumes that the reader is familiar with the FATCA regulations and is experienced with extensible markup language (XML) and schema technology.

DRAFT

Document	Description
FATCA Online Registration User Guide (Publication 5118)	Provides instructions for the online system to complete an electronic Form 8957, FATCA Registration
FFI List Search and Download Tool User Guide (Publication 5147)	Provides instructions on how to use the FFI List Search and Download Tool to search for an approved GIIN
FATCA XML Schema v1.1 User Guide (Publication 5124)	Explains the information required to be included in each data element of the schema
FATCA Sender Metadata Schema v1.0 User Guide (Publication 5188)	Explains the schema and elements of a FATCA metadata file
Instructions for Form 8966, FATCA Report	Provides instructions for the paper Form 8966, FATCA Report

Table 1- FATCA Related Documents List provides a list of related FATCA publications.

Comments

We appreciate your feedback on the quality and usefulness of this publication. Please send comments, with a reference to chapter, section, and page number(s), to lbi.fatca.ides@irs.gov.

Technical Support

IDES technical assistance is available Monday through Friday, 24 hours a day, except for U.S. federal holidays, through the IDES Customer Service Help Desk. IDES customer support will send a system alert from the help desk portal for planned outages and scheduled maintenance.

2. International Data Exchange Service (IDES)

About IDES

The IDES web application is a secure managed file transfer service that is available to both FIs and HCTAs to facilitate FATCA reporting. This reporting is provided for under U.S. Treasury Regulations, the FFI agreement, Tax Information Exchange Agreements (TIEAs), Intergovernmental Agreements (IGAs), and other guidance issued by the Treasury Department and the IRS that outlines how financial institutions will implement FATCA. The data collected through IDES will be incorporated into IRS compliance operations.

IDES is accessible to enrolled users over the Internet via Hypertext Transfer Protocol Secure (HTTPS) or Secure File Transfer Protocol (SFTP). IDES provides for an end-to-end controlled file transfer with enhanced monitoring and security features. The system only accepts encrypted electronic submissions, and will allow for the transmission of FATCA reporting in the approved FATCA XML Schema v1.1 (FATCA XML). For more information on FATCA regulations, Form 8966 and instructions, FATCA XML, and other related topics, visit the FATCA Home Page.

The main function of IDES is to provide authorized users with secure exchange services for FATCA data transmissions, with the additional protection of a Public Key Infrastructure (PKI). The primary features of IDES are:

- Enrollment
- Certificate Management
- Account Management
- Secure Data Transmission
- Status of Data Transmission (Alerts and Notifications)

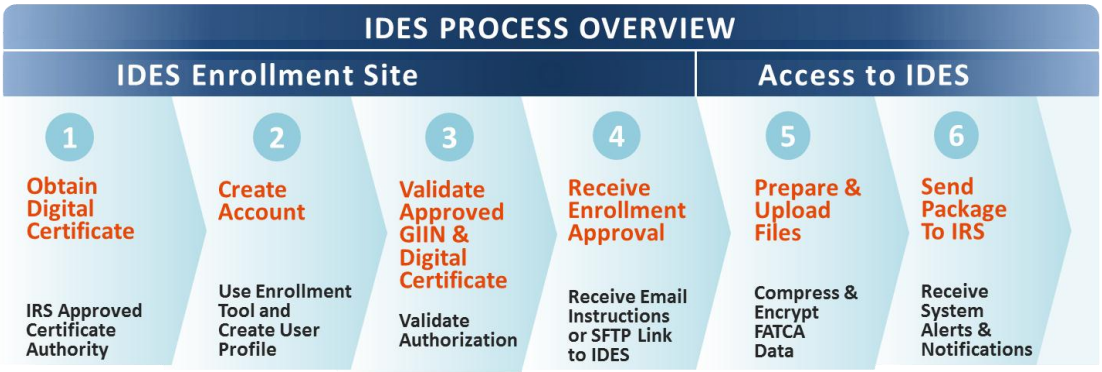


Figure 1: IDES Process Overview describes the overall process for enrolling in IDES and sending data to the IRS.

DRAFT

Before You Begin

This material is intended to supplement the contents of IDES online help and is not intended to replace technical documentation to establish and test SFTP connections. Examples shown in this document are based upon a Windows environment and may differ if using other operating systems.

Icon	Description
Bold	Bold text is used in steps to denote buttons or menu options intended to be clicked or selected
Emphasis	References to sections within this document
ISO Country Codes	Review the list of ISO country codes, 3-digit number
Printing	Use internet browser print option to print directly from IDES

Table 2 - Conventions to describe the graphics used throughout this guide.

Authorized Users

Authorized IDES users are either FIs or HCTAs. Each authorized user has limited access to the system based on the data flow model described in their agreement with the United States (for example, an IGA or an FFI agreement) or in Treasury regulations. Note that for many IDES users, the IRS is the only valid recipient for files. The table below provides additional information regarding user access based on agreement types.

Type of Agreement	User Type	Access Description
Model 1 IGA (Non-Reciprocal) FFI transmits data directly to its HCTA then the HCTA transmits data to the IRS	FFI	No Access
	HCTA	On behalf of FFI under the HCTA jurisdiction: ▪ Upload FATCA reporting for direct transfer to IRS ▪ Download alerts generated by IDES ▪ Download notifications and Competent Authority Requests (CARs) submitted by IRS
Model 1 IGA (Reciprocal) FFI transmits data directly to its HCTA then the HCTA transmits data to the IRS. This is a reciprocal model with two-way transmission between the HCTA and the IRS	FFI	No Access
	HCTA	On behalf of FFI under the HCTA jurisdiction: ▪ Upload FATCA reporting for direct transfer to IRS ▪ Download alerts generated by IDES ▪ Download notifications and CARs submitted by IRS Reciprocal data will be exchanged with HCTA
Model 1 Option 2 FFI transmits data directly to its HCTA via IDES. The HCTA approves or rejects the FATCA reporting data. If approved, IDES releases the data to the IRS.	FFI	Upload FATCA reporting to IDES for review by HCTA Download alerts generated by IDES Download notifications submitted by IRS (subject to the terms of the country's IGA)
	HCTA	Upload approved or rejected FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications and CARs submitted by IRS
Model 2 IGA and FFI agreement FFI transmits data regarding: ▪ Consenting accountholders directly to IRS, ▪ Aggregate information on non-consenting accountholders and non-consenting non-participating FFIs directly to IRS, and ▪ Specific information on non-consenting accountholders and non-consenting non-participating FFIs directly to HCTA. HCTA may deliver data to IRS after a treaty request	FFI	Upload FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications submitted by IRS (subject to the terms of the country's IGA)
	HCTA	Upload FATCA reporting regarding non-consenting accountholders and non-consenting non-participating FFIs for direct transfer to IRS (after treaty request) Download alerts generated by IDES Download notifications and CARs submitted by IRS
Non-IGA (FFI agreement) FFI transmits data directly to the IRS	FFI	Upload FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications submitted by IRS

DRAFT

	HCTA	No Access

Table 3 - Table Valid User Types and Features summarizes IDES access, data flow and functionality based on valid user type and model. Some entities are eligible to enroll on behalf of themselves and their branches.

System Availability

The IDES system requires a username and password, which can be obtained through the IDES enrollment process. The system will be available 24 hours a day, with the exception of U.S. holidays and regularly scheduled system maintenance periods. All users will be notified of planned and unplanned outages that could affect data transfers.
IDES works with all major browsers and can be accessed using different FTP clients for Secure File Transfer Protocol (SFTP).

Items	Technical Specifications
Browsers for HTTPS	▪ Apple Safari 5.0 on OS X only ▪ Google Chrome 33.x or later ▪ Microsoft Internet Explorer 9, 10, 11 (IE 8 and Compatibility View are not currently supported) ▪ Mozilla Firefox 29 or later
FTP clients for SFTP	▪ Axway Secure Client 5.8, 6.0, 6.1 ▪ cURL 7.19 to 7.22 ▪ FileZilla Client 3.5.x ▪ PSCP 0.60 ▪ PSFTP 0.60 ▪ Tectia Client 6.1, 6.2 ▪ VanDyke SecureFX 6.6.1 to 6.7 ▪ WinSCP 4.2.9 to 4.3.5
JavaRuntime Environment	▪ JRE 1.6 or later
JavaScript	▪ Enabled ▪ Cookies enabled
File Size	▪ File uploads and downloads are limited to a size of 200 MB compressed.
File Naming Conventions	▪ See Section *Preparing the FATCA XML* for file naming conventions. ▪ Only file extension .zip are authorized for file uploads to IDES in the user Outbox folders ▪ File names are case insensitive ▪ Do not use illegal characters in the name of files, such as colon, backslash, question mark or space

Table 4 - System Requirements provide an overview of browsers and connections that have been successfully tested with IDES. Other similar technologies may work with IDES but have not been tested and therefore are not officially supported.

Note: Axway Secure Transport Web Access Plus (508-compliant WebUI) requires JRE 1.6 or later.

Data Security

DRAFT

IDES provides secure file data transfers by using symmetric and asymmetric encryption schemes to encode data. IDES uses the Advanced Encryption Standard (AES), a specification for encryption of electronic data established by the United States National Institute of Standards and Technology (NIST).

When a supported web browser connects to IDES via HTTPS, the Transport Layer Security (TLS) cryptographic protocol provides communication security over the Internet and the session is encrypted for data confidentiality. When a supported FTP client connects to IDES via SFTP, the Secure Shell (SSH) network protocol provides secure file transfer functionality over a reliable data stream. The IDES Enrollment website requires account authentication through the use of strong passwords. Files cannot be opened, read, or decrypted at any point during data transmission.

File Retention

IDES provides secured temporary file storage for data transmissions; however, IDES is not a data storage service. IDES file retention policy states that each file transmitted remains available for download in the recipient's account inbox folder for a period of 7 days. If the recipient does not download the file within 7 days, the files expires and will be deleted. For this reason, expired files cannot be downloaded.

If the recipient initiates the download of a file within 7 days, that file will remain available for download for only 24 hours from the time the download is initiated. After 24 hours the file expires and will be deleted. Note that an inbox folder may contain several different transmitted files at the same time, each with a different payload. For the purpose of this document, the term payload will be used to describe the body of the data packet (e.g. a FATCA XML document) that serves as the fundamental purpose of the data transmission.

Any files with errors, such as files with an unencrypted payload or infected with a virus, will be deleted immediately.

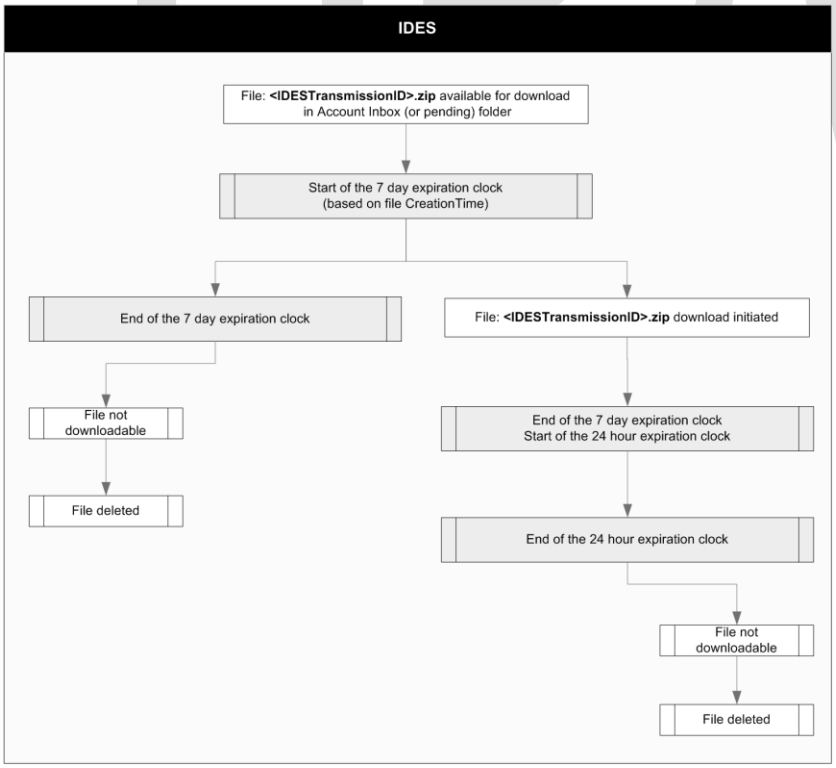


Figure 2- File Retention Flow shows the process to delete files from IDES

Requirements

DRAFT

Certain requirements are needed to create a new account on the IDES Enrollment site. Requirements differ for HCTA and FI users.

Valid User Type		
Requirements	**HCTA**	**FI**
Registered GIIN See *IRS FFI List* for more information	N/A	X
HCTA GIIN pre-assigned username	The IRS provided usernames to your Competent Authority. Contact the IRS for more information	N/A
Valid certificate issued by an IRS approved certificate authority (CA) See Section, *Obtaining a Certificate*	X	X
Public and Private Key	X	X
Email address of additional users	X	X

Table 5- IDES Enrollment Requirements provides an overview of information needed to use the enrollment portal.

Note: For FIs that do not have a requirement to obtain a GIIN, a separate web link will direct user to a modified Enrollment page. For information on how to obtain a GIIN, refer to the FATCA Online Registration System User Guide.

HCTA Username and Password

All countries under Model 1 IGAs have a pre-assigned username and HCTA GIIN. Each HCTA GIIN is in the format: **000000.00000.TA.<ISO>**. ISO is the ISO 3166-1 numeric standard country code. The first time a user logs on to IDES, the user is required to change its assigned username and create a password. A letter containing information on the username and enrollment instructions will be sent to an appropriate contact from each country based on their agreement with the United States. For additional information, contact FATCA IDES at lbi.fatca.ides@irs.gov.

3. Obtaining a Digital Certificate

Purpose of a Digital Certificate

Certificates and their related private keys are used to sign and decrypt messages between the sending party and the IRS. A digital certificate binds an identity to a public key. Certificate Authorities (CA) issue certificates after an identity proofing process to verify the certificate owner. The individual identified in the certificate has possession and control over the private key associated with the public key found in the certificate.

IRS Approved Certificate Authorities

The IRS only accepts certificates issued by approved CAs. A published list of certificate authorities and acceptable digital certificate products is available on IRS.gov.

Certificate Authority	Type of Certificate	External Website Links
DigiCert	SSL Plus (Single Name)	https://www.digicert.com/welcome/ssl-plus.htm
Entrust	Standard SSL	http://www.entrust.net/ssl-certificates/standard.htm
GlobalSign	Organization SSL	https://www.globalsign.com/ssl/organization-ssl/
IdenTrust	TrustID Server (SSL)	https://www.identrust.com/certificates/buy_trustid_server.html
StartCom	StartSSL EV	https://www.startssl.com/?app=30
Symantec/Verisign	Secure Site SSL	http://www.symantec.com/ssl-certificates/secure-site/?inid=vrsn_symc_ssl_SS
Thawte	SSL Web Server	http://www.thawte.com/ssl/web-server-ssl-certificates/index.html

Table 6 - Certificate Authorities summarizes a list of IRS-approved CAs.

Upload a Digital Certificate to IDES

After an FI or HCTA administrator obtains a digital certificate, the user will provide the certificate to IDES during the enrollment process. Upon upload, the certificate is validated with the Certificate Authority (CA) that issued the certificate. IDES stores the certificate and makes it available to other IDES users who will use it to verify digital signatures and encrypt symmetric key files. It is the responsibility of IDES users to verify that the certificate is still valid at the time they attempt to use it.

Public Key Certificate

A public key certificate, also known as a digital certificate, is an electronic document used to prove ownership of a public key. The IRS public key certificate can be downloaded during IDES enrollment. The Administrator will upload the digital certificate for its FI or HCTA during enrollment. All public keys or certificates are made available for all IDES users.

Certificate Maintenance

IDES uses a Public Key Infrastructure (PKI) to manage and revoke digital certificates. The CA sets the lifetime of each digital certificate, typically up to one year. IDES requires one digital certificate per FI or HCTA.

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked, meaning that they are not trustworthy, and should not be used. CRLs are always issued by the trusted CA and are publicly available. IDES validates all digital certificates against the most current CRL published from each trusted CA to identify any revoked digital certificates. A revoked digital certificate will be deleted from IDES, along with the associated public key contained in the digital certificate. IDES will immediately deactivate the user account associated with a revoked digital certificate.

The Online Certificate Status Protocol (OCSP) is an Internet protocol designed for real-time verification of digital certificates against a database of revoked digital certificates. IDES tests all digital certificates using the OCSP to verify whether the digital certificates are valid. For example, when a transmission uses an expired digital certificate, IDES tests the certificate using the OCSP, confirms the certificate is revoked, and deletes the transmitted file. Users are not able to transmit the file until a valid digital certificate is resubmitted.

4. IDES Enrollment

Overview

IDES Enrollment is required for FIs and HCTAs to access the IDES environment. Users must enter a valid GIIN and certificate to enroll. FIs or HCTAs with invalid or expired certificates cannot enroll.

IDES Enrollment Options:

- Add, Update and Delete a User
- Update Certificate
- Disable/Enable a User
- Select Alert Preferences
- Create Metadata File

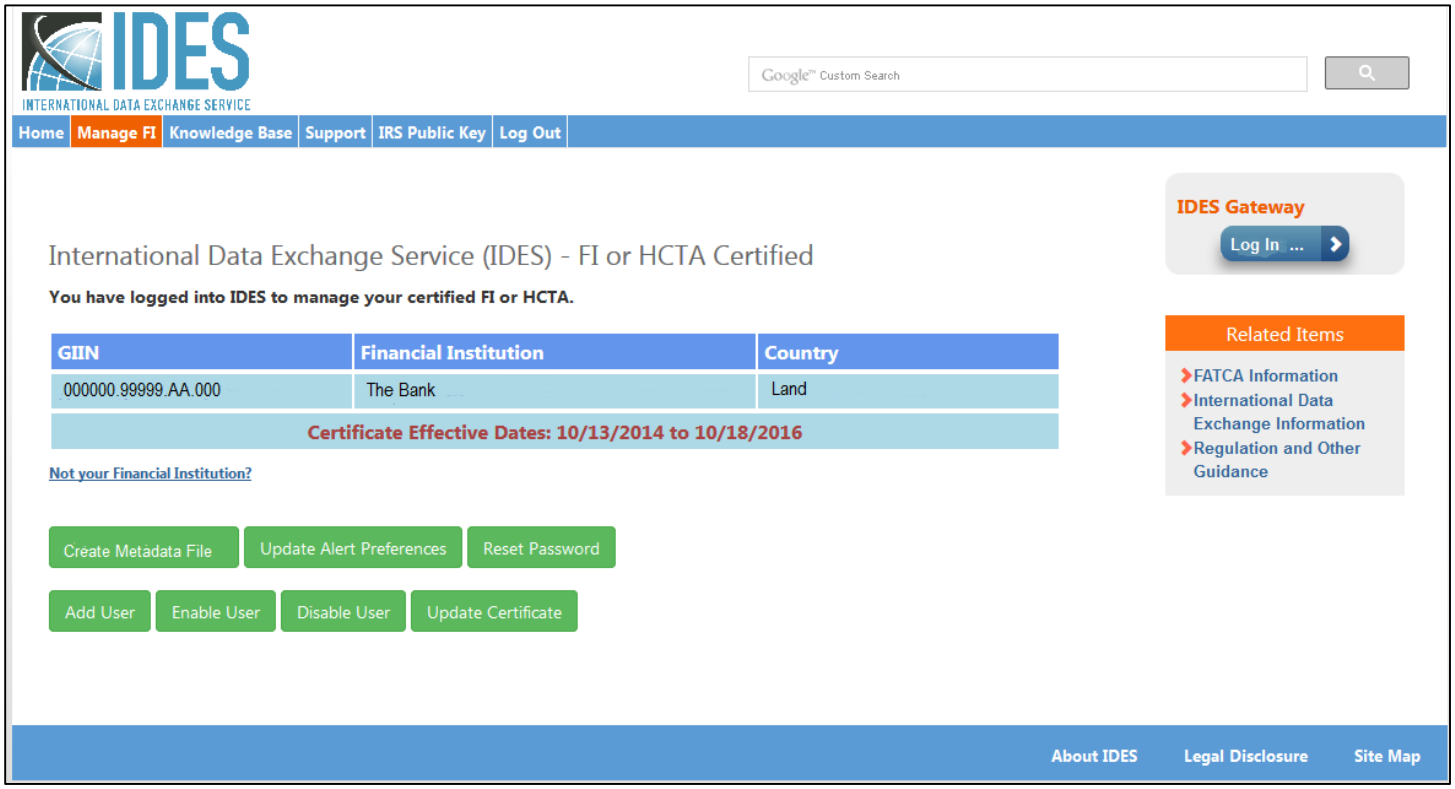


Figure 3

Accessing the IDES Enrollment Site

IDES Enrollment Home Page

The IDES Enrollment site is a secure, web based system available 24 hours per day, Monday through Friday, with the exception of regularly scheduled maintenance. Users will be notified of any unplanned outages that are expected to last more than 8 hours. The IDES Enrollment site can be accessed through:

- IDES Enrollment Web User Interface
- Secure File Transfer Protocol (SFTP)

The IDES Enrollment site contains links to various IDES resources and includes five main tabs in addition to the Home tab:

1. Enrollment
2. Knowledge Base
3. Support
4. IRS Public Key
5. IDES Enrollment User Log In

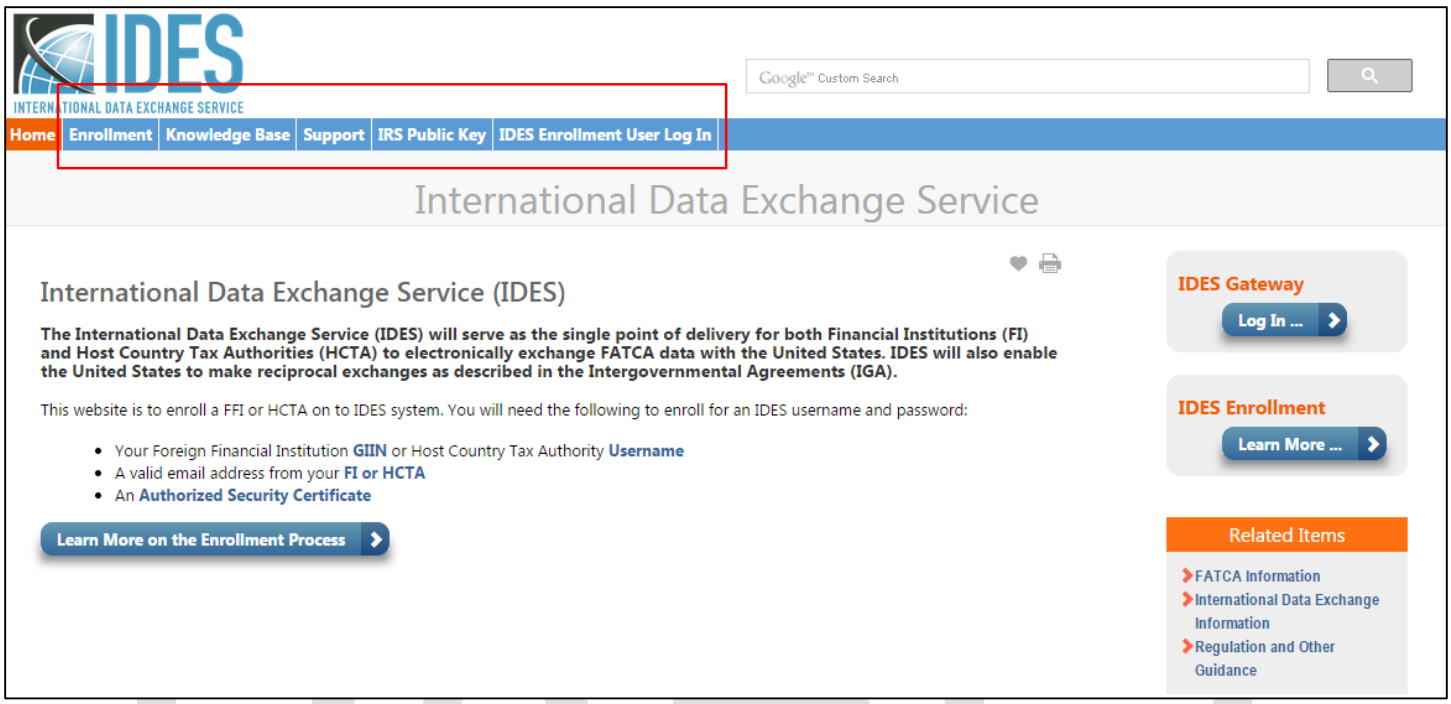


Figure 4

DRAFT

Enrollment Tab

The Enrollment tab describes the IDES enrollment process and provides users with access to create an IDES account. The Enrollment tab also links to the IDES Gateway, a web application that allows enrolled HCTAs and FIs to securely upload and download FATCA data over the Internet using both HTTPS and SFTP protocols.

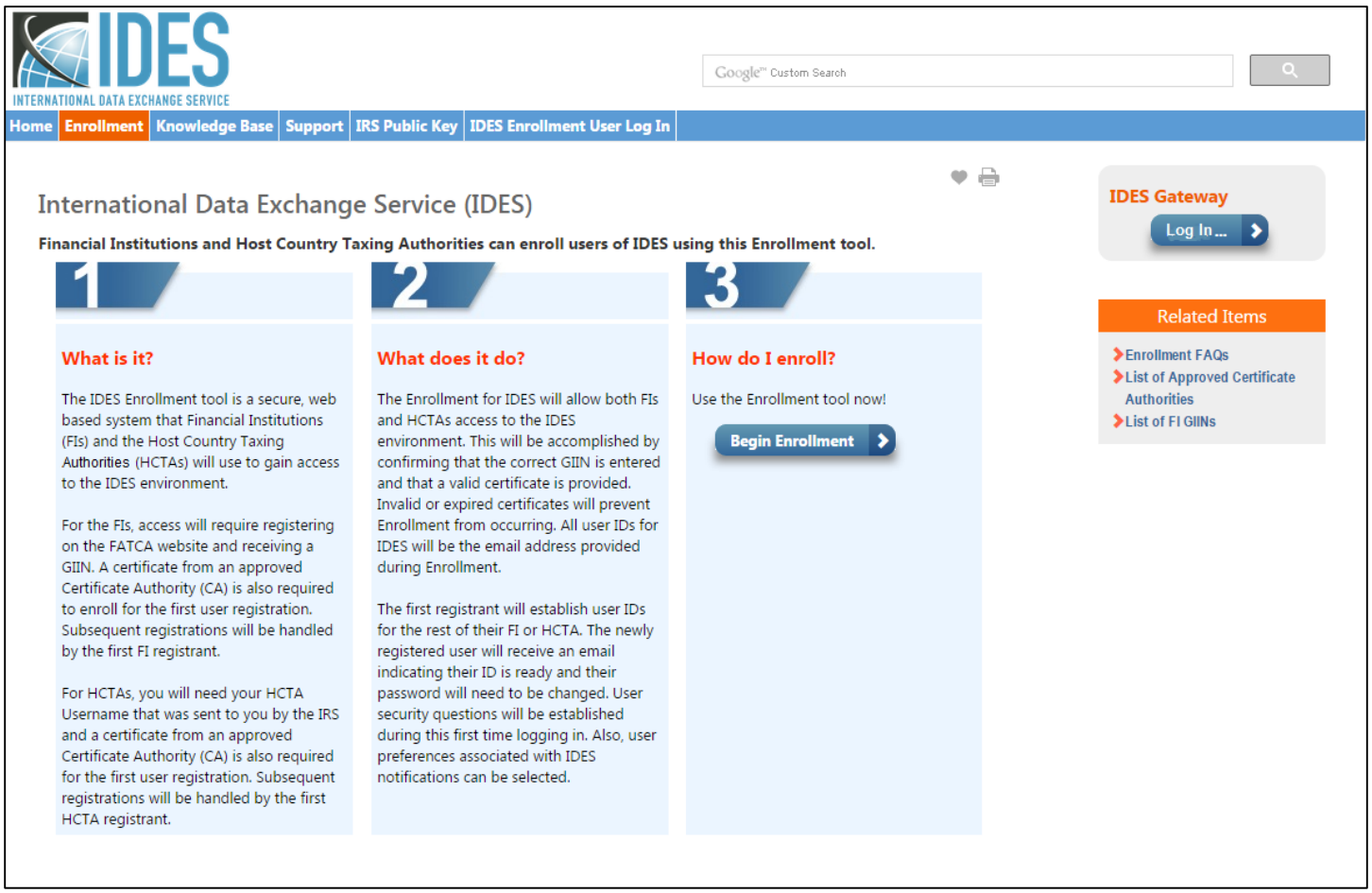


Figure 5

Knowledge Base Tab

The Knowledge Base tab directs users to important IDES documentation such as user guides and an interactive knowledge base.

Users can access the following resources from the Knowledge Base tab:

- Interactive IDES Knowledge Base
- IDES User Guides
- IDES Frequently Asked Questions (FAQs)

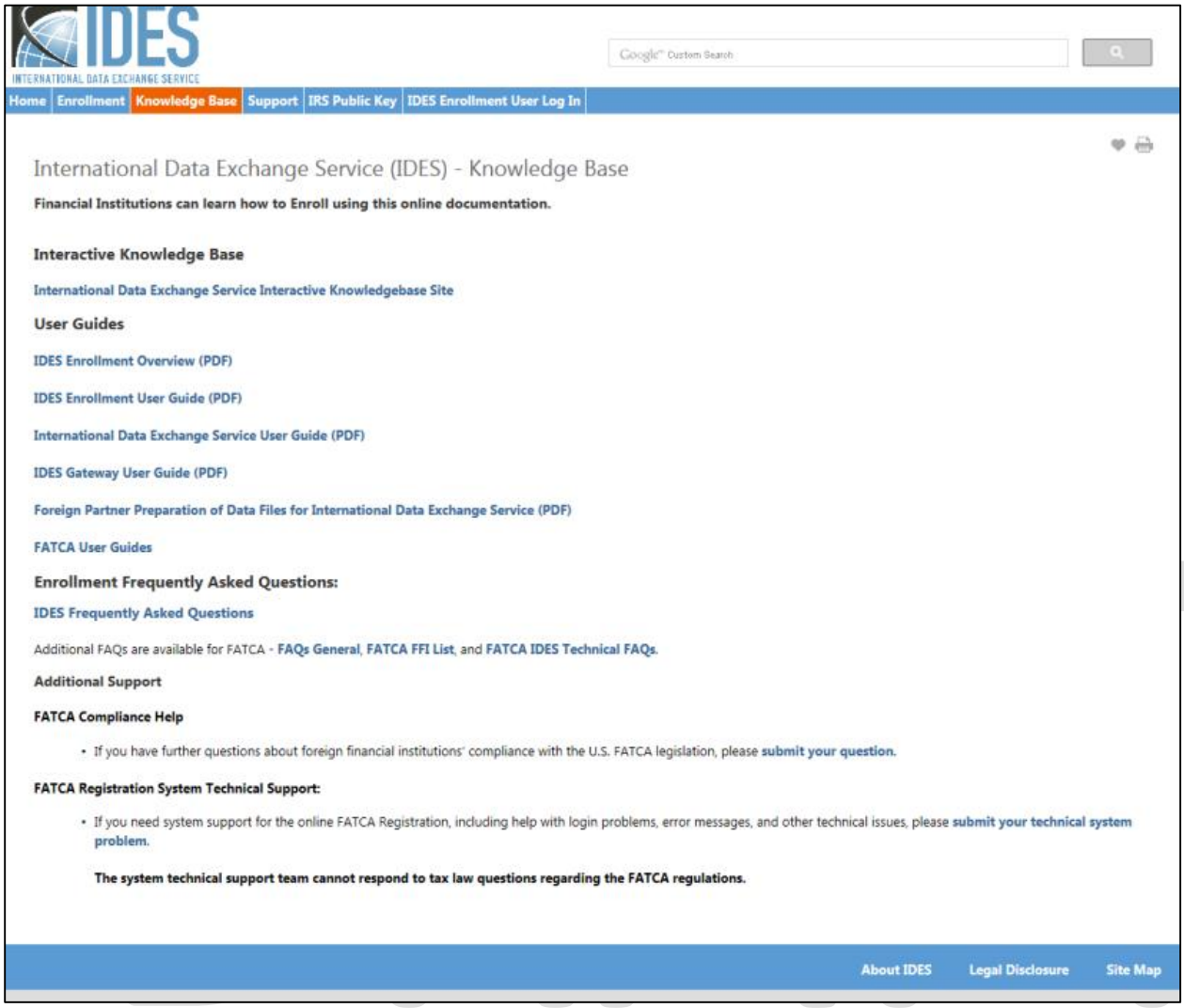

IDES
INTERNATIONAL DATA EXCHANGE SERVICE
Google™ Custom Search
Home
Enrollment
Knowledge Base
Support
IRS Public Key
IDES Enrollment User Log In
International Data Exchange Service (IDES) - Knowledge Base
Financial Institutions can learn how to Enroll using this online documentation.
Interactive Knowledge Base
International Data Exchange Service Interactive Knowledgebase Site
User Guides
IDES Enrollment Overview (PDF)
IDES Enrollment User Guide (PDF)
International Data Exchange Service User Guide (PDF)
IDES Gateway User Guide (PDF)
Foreign Partner Preparation of Data Files for International Data Exchange Service (PDF)
FATCA User Guides
Enrollment Frequently Asked Questions:
IDES Frequently Asked Questions
Additional FAQs are available for FATCA - FAQs General, FATCA FFI List, and FATCA IDES Technical FAQs.
Additional Support
FATCA Compliance Help
• If you have further questions about foreign financial institutions' compliance with the U.S. FATCA legislation, please submit your question.
FATCA Registration System Technical Support:
• If you need system support for the online FATCA Registration, including help with login problems, error messages, and other technical issues, please submit your technical system problem.
The system technical support team cannot respond to tax law questions regarding the FATCA regulations.
About IDES
Legal Disclosure
Site Map

Figure 6

Support Tab

The IDES help desk is available to assist users with log in problems, error messages, and other technical issues. The Support tab provides contact information for the help desk and hours of operation. The help desk can be contacted by phone or via an online form which allows users to submit technical system problems. Please note that the help desk is available in English only.

Users can access the following resources from the Support tab:

- Email Support
- Phone Support
- Help Desk Hours of Operation
- Submit Technical System Problems

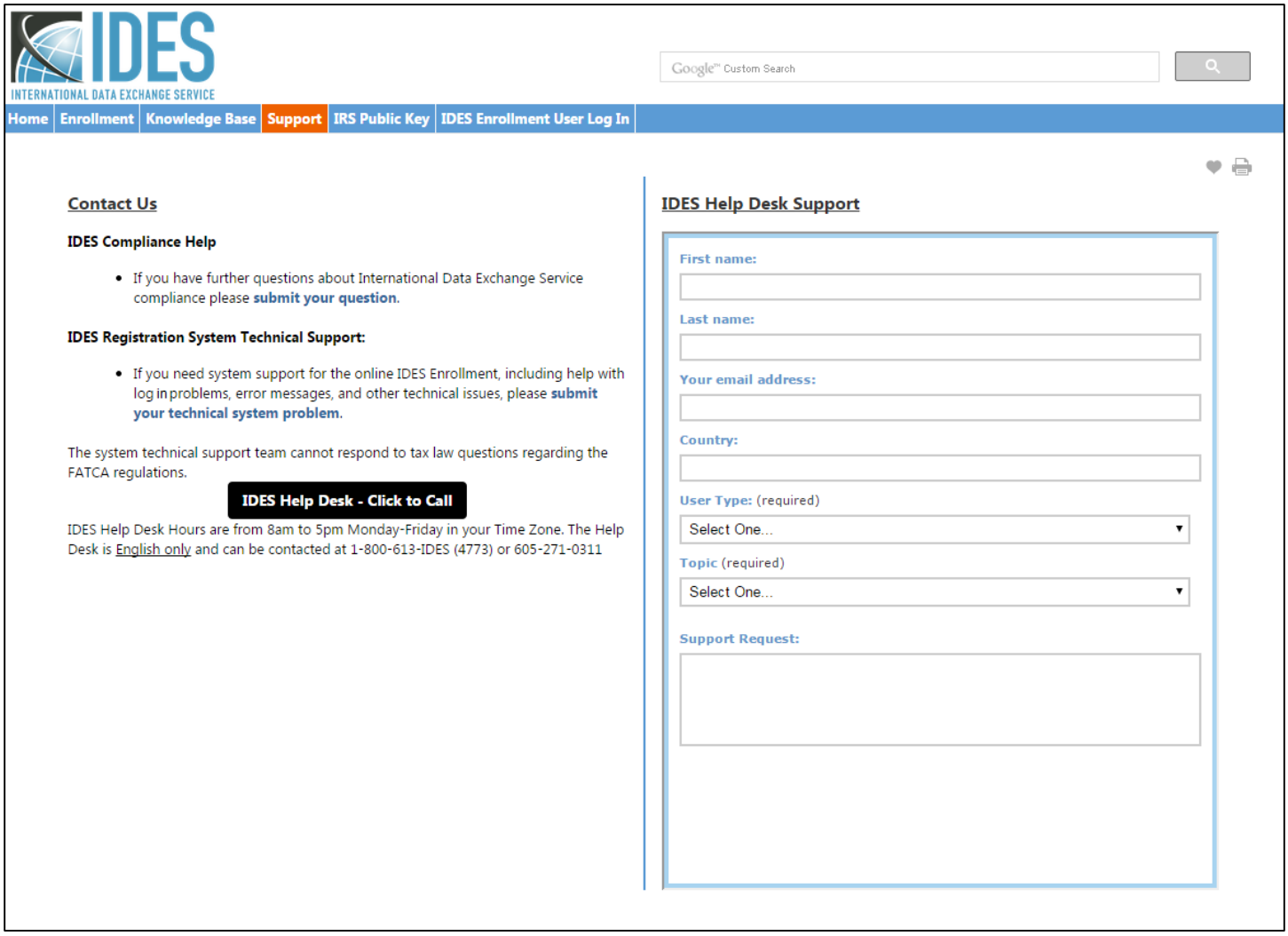


Figure 7

IRS Public Key Tab

The IRS Public Key is a certificate that can be downloaded from the IDES Enrollment site. This certificate should be included in the FATCA transmission archive transmitted to the IRS.

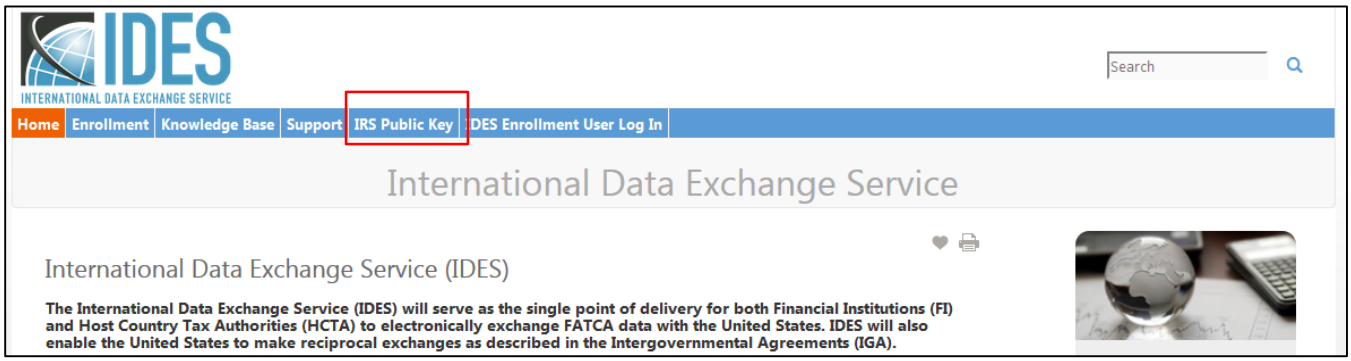


Figure 8

1. From the IDES Support home page, click the **IRS Public Key** tab.

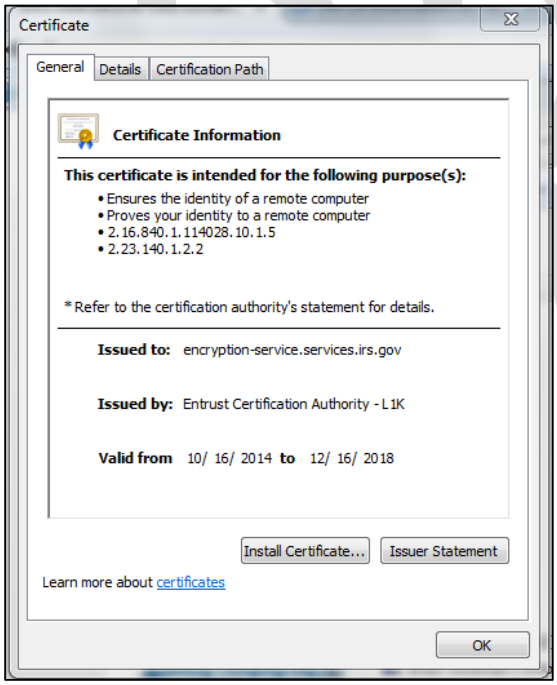


Figure 9

2. Download and save the IRS Public Key Certificate to your computer.
3. The certificate should be included in the transmission archive .zip file transmitted to the IRS via the IDES Gateway.

IDES Enrollment User Log In Tab

The IDES Enrollment User Log In tab allows returning users to access the IDES Enrollment site. HCTA Administrators, FI Administrators, and end users are able to log in after they have created an IDES account.

DRAFT

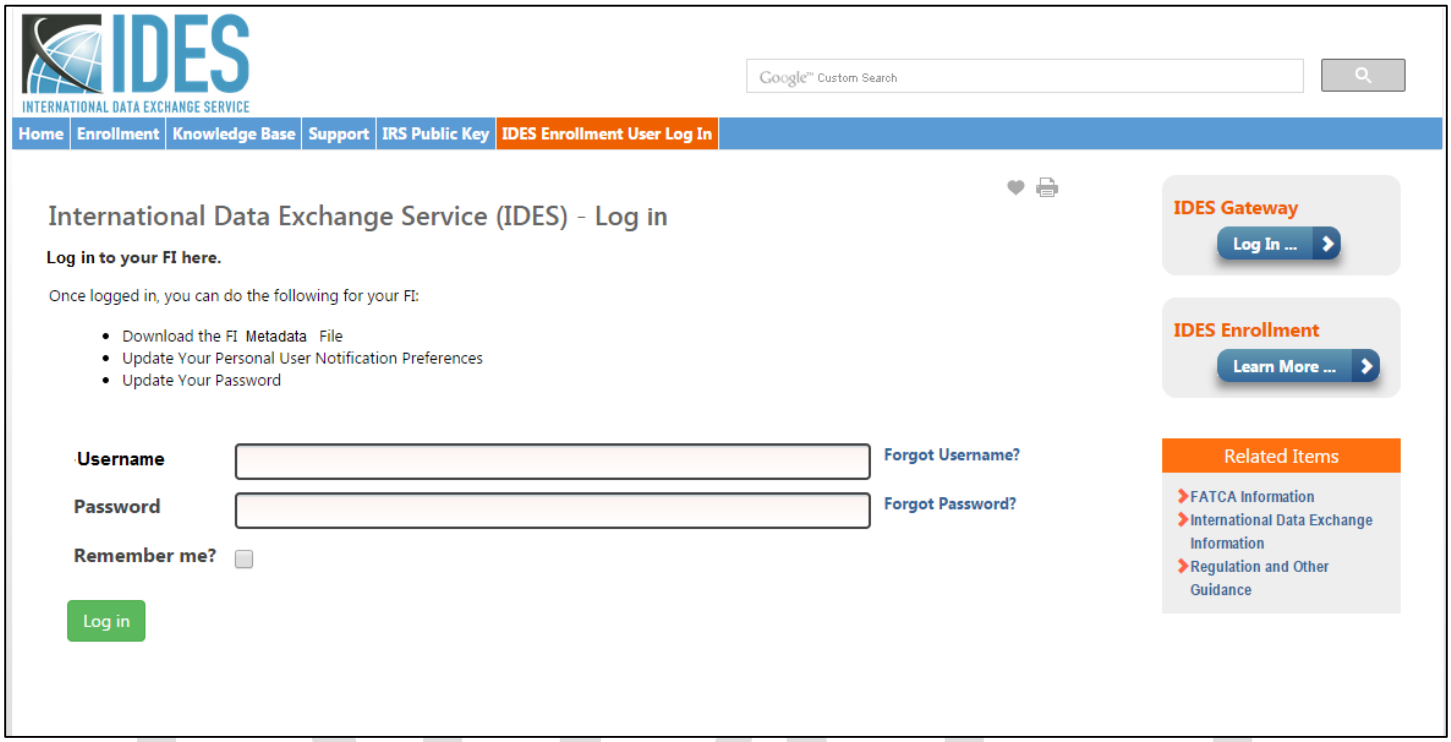


Figure 10

DRAFT

5. HCTA Administrators

Overview

HCTAs will play the following roles under the IGAs:

- **Model 1 IGA HCTA:** The partner jurisdiction agrees to report to the IRS specified information about the U.S. accounts maintained by all relevant FIs located in the jurisdiction.
- **Model 2 IGA HCTA:** The partner jurisdiction agrees to direct and enable all relevant FIs located in the jurisdiction to report specified information about their U.S. accounts directly to the IRS.

HCTAs will need their IRS assigned username in order to create an IDES account. The first user that registers for an IDES account, on behalf of their HCTA, is considered the Administrator. HCTA Administrators are able to add end users, disable and enable end users, update the certificate, update alert notifications, create a metadata file, reset passwords, and download the IRS Public Key.

Authorized end users (users under the HCTA Administrator) have limited capabilities and may update their alert notifications, create a metadata file, and reset their password.

To create an account, the HCTA Administrator will create challenge questions and a password. The HCTA Administrator will then upload their digital certificate received from an IRS approved certificate authority.

DRAFT

Begin Enrollment

The IDES Enrollment site can be accessed at https://www.ides-support.com.

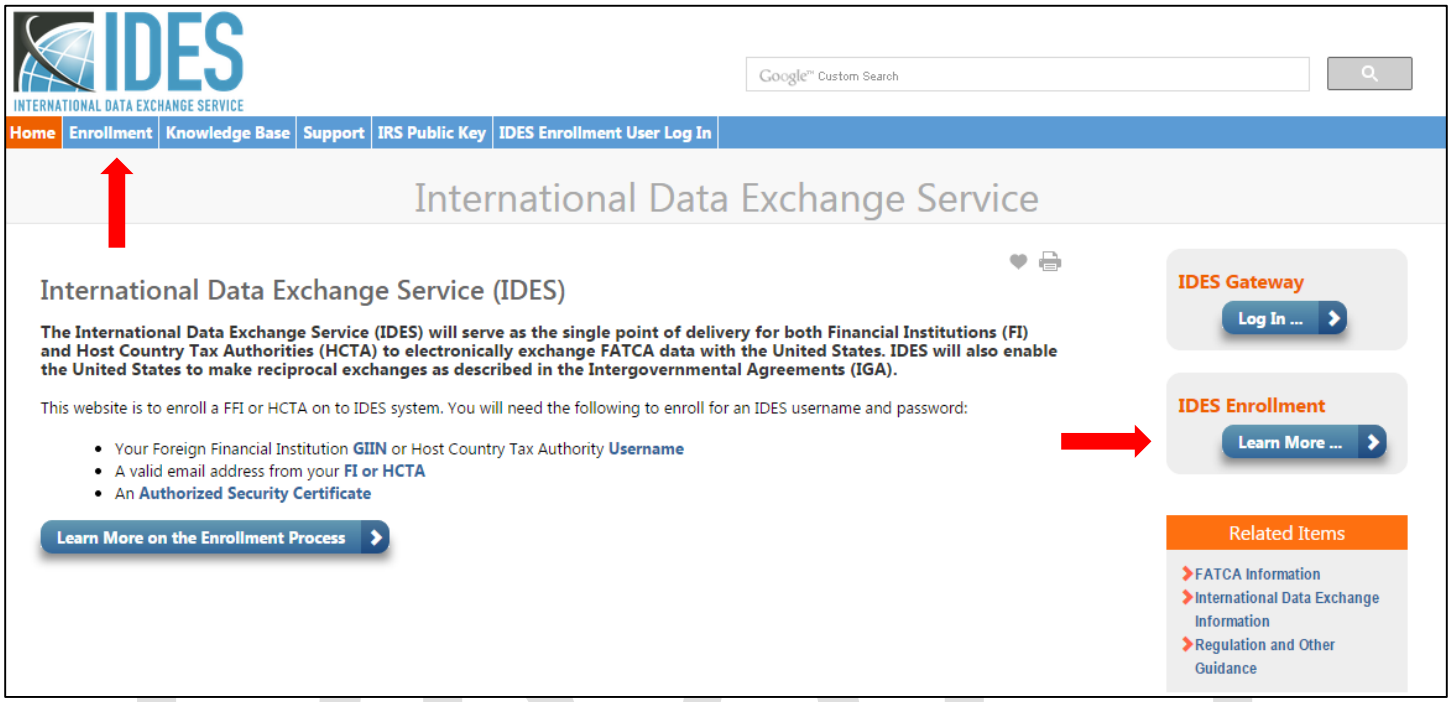


Figure 11

1. Click **Learn More** under IDES Enrollment or the **Enrollment** tab.

DRAFT

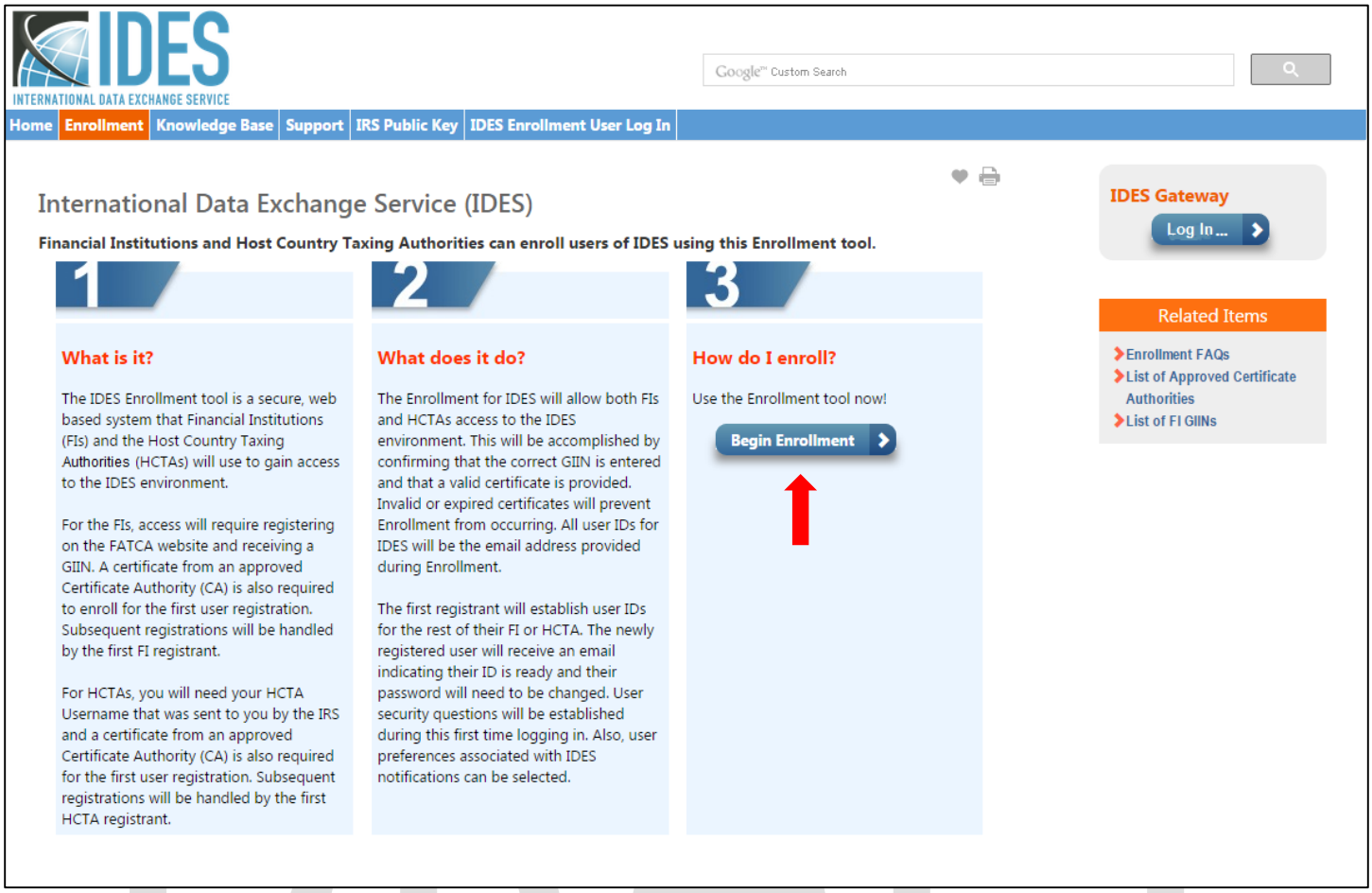


Figure 12

2. Click on **Begin Enrollment** to start the enrollment process as an HCTA Administrator.

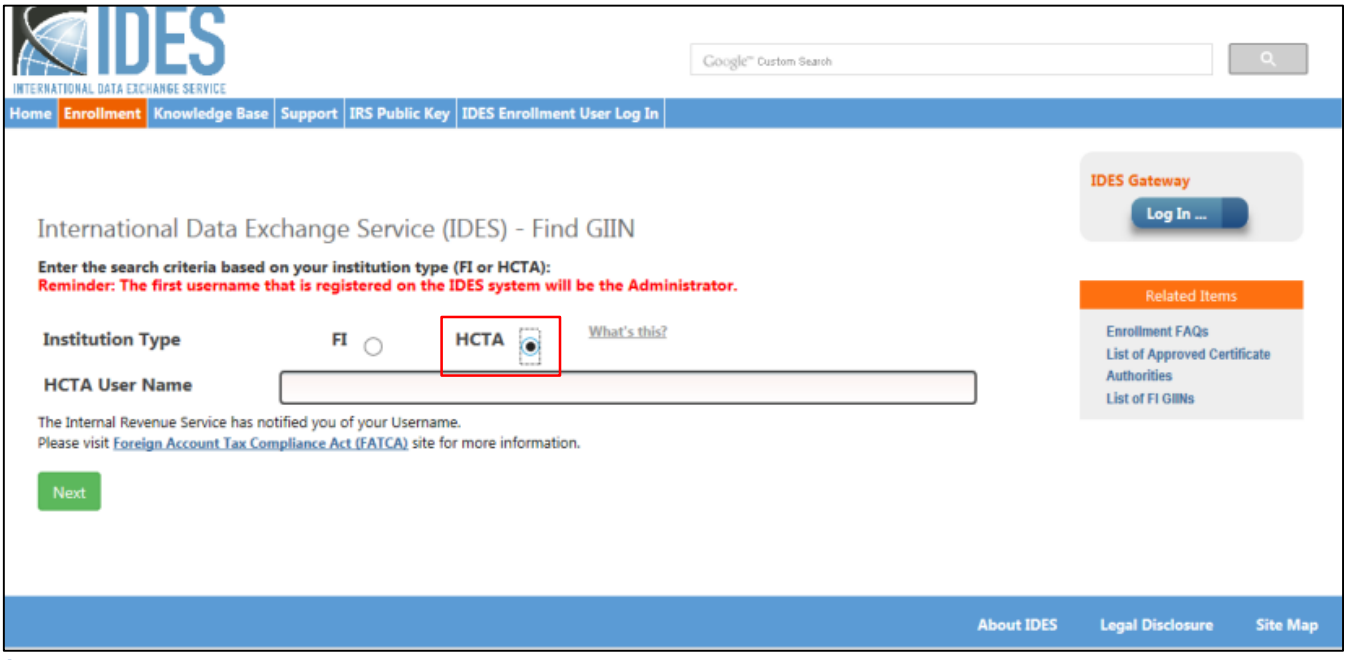


Figure 13

3. Select **HCTA**.

4. In **HCTA Username**, enter your pre-assigned username. If you have not received an HCTA username contact your local Competent Authority or IDES customer support.
5. Click **Next** to continue.

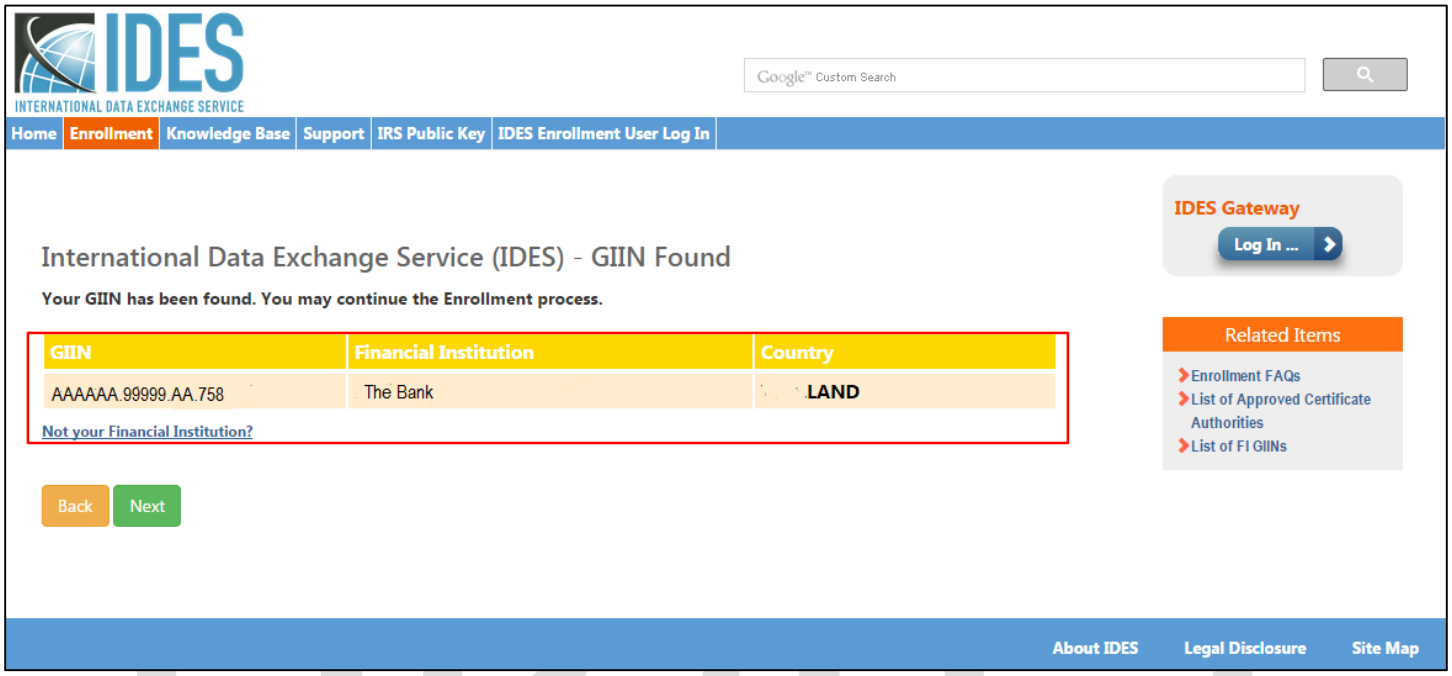


Figure 14

6. Confirm information and verify **GIIN**, **Financial Institution**/HCTA and **Country** are correct.
7. Click **Next** to continue and set up **Challenge Questions**

DRAFT

Create Challenge Questions

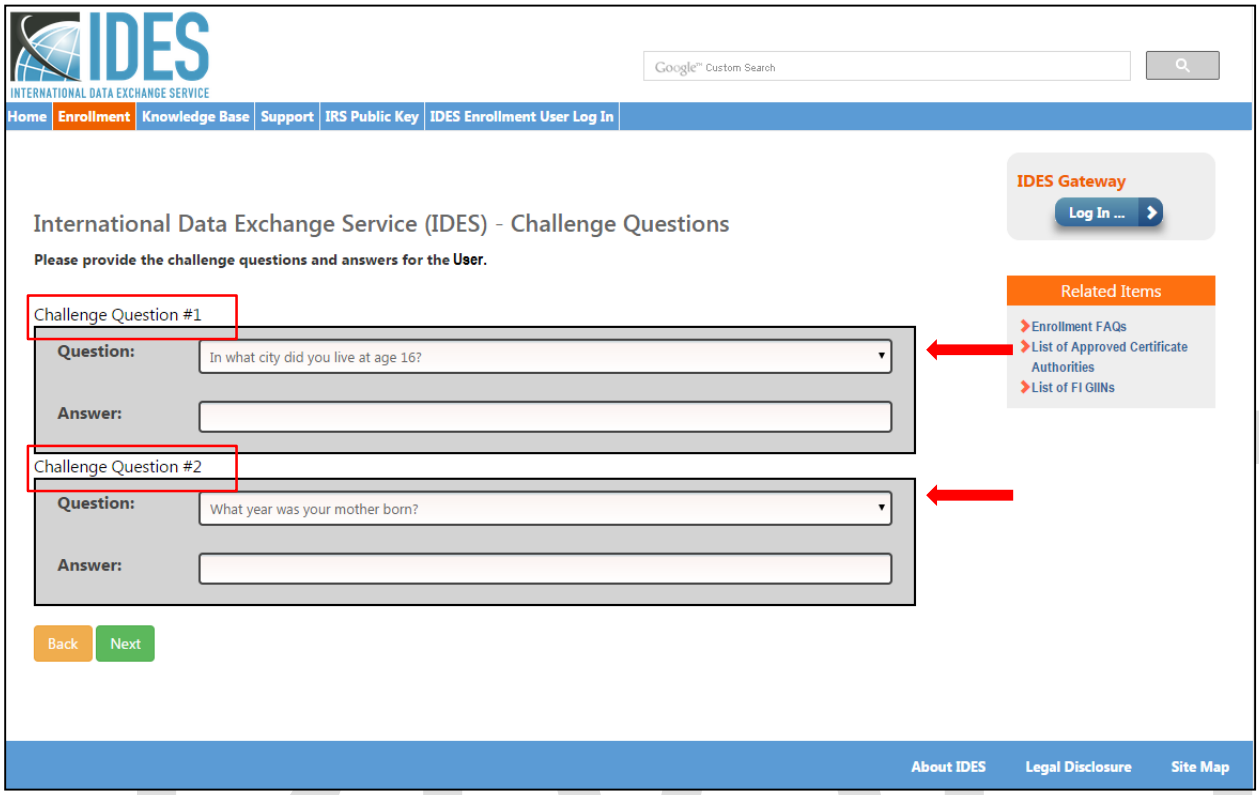


Figure 15

1. **Challenge Question #1**
   a. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   b. Answer: Type a response to the challenge question.
2. **Challenge Question #2**
   a. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   b. Answer: Type a response to the challenge question.
3. Click **Next** to continue and set up a **Username**

IMPORTANT: Remember to document your answers to your challenge questions. Users will need these answers to reset a password or to contact the IDES Help Desk.

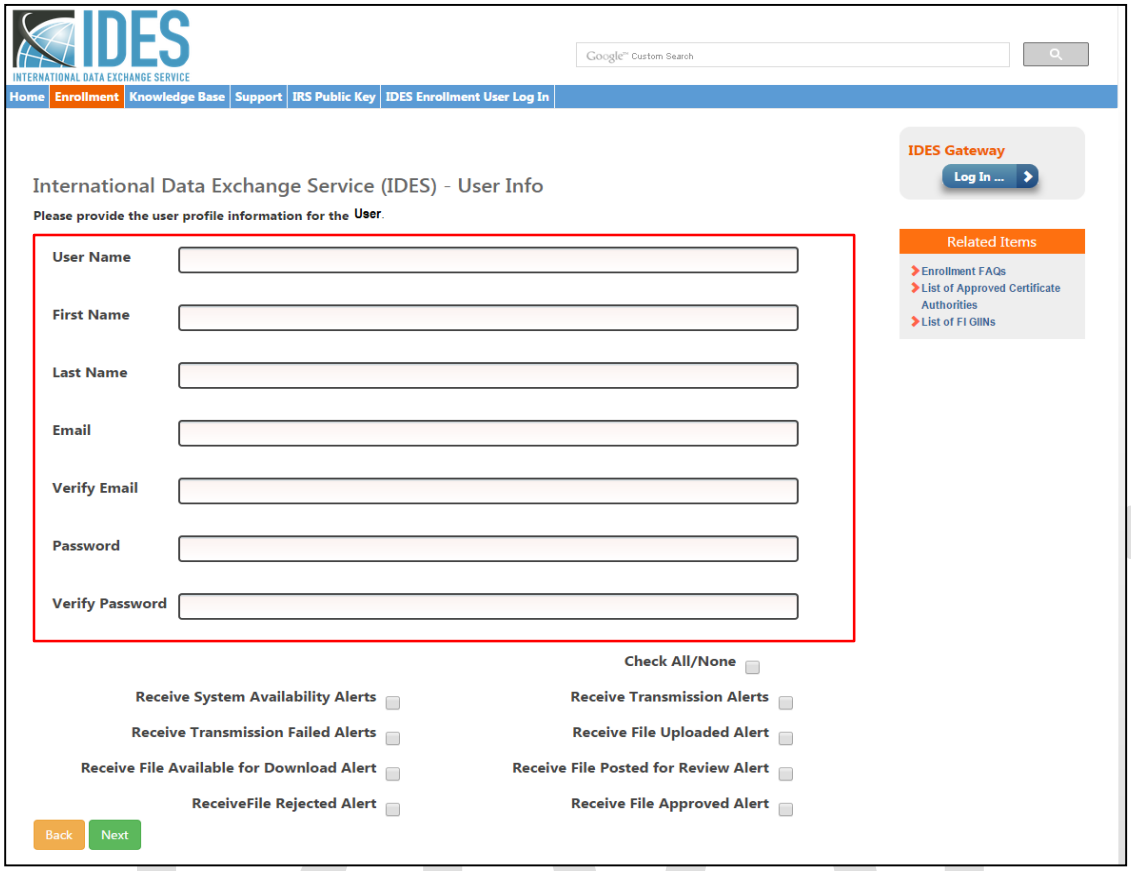


Figure 16

1. **Username** – Enter your new username. We recommend first initial and last name. If the username is already taken you will receive an error message.
2. **First Name** – Enter your first name.
3. **Last Name** – Enter your last name.
4. **Email** – Enter your email address.
5. **Verify Email** – Enter your email address again (must match the previous entry). If it does not match, you will receive an error message.
6. **Password** – Create a valid password.
    a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .).
    b. If you enter a password that does not meet the guidelines, you will receive an error message.
7. **Verify Password** – Re-type your password (must match the previous entry). If it does not match, you will receive an error message

Select Alert Preferences

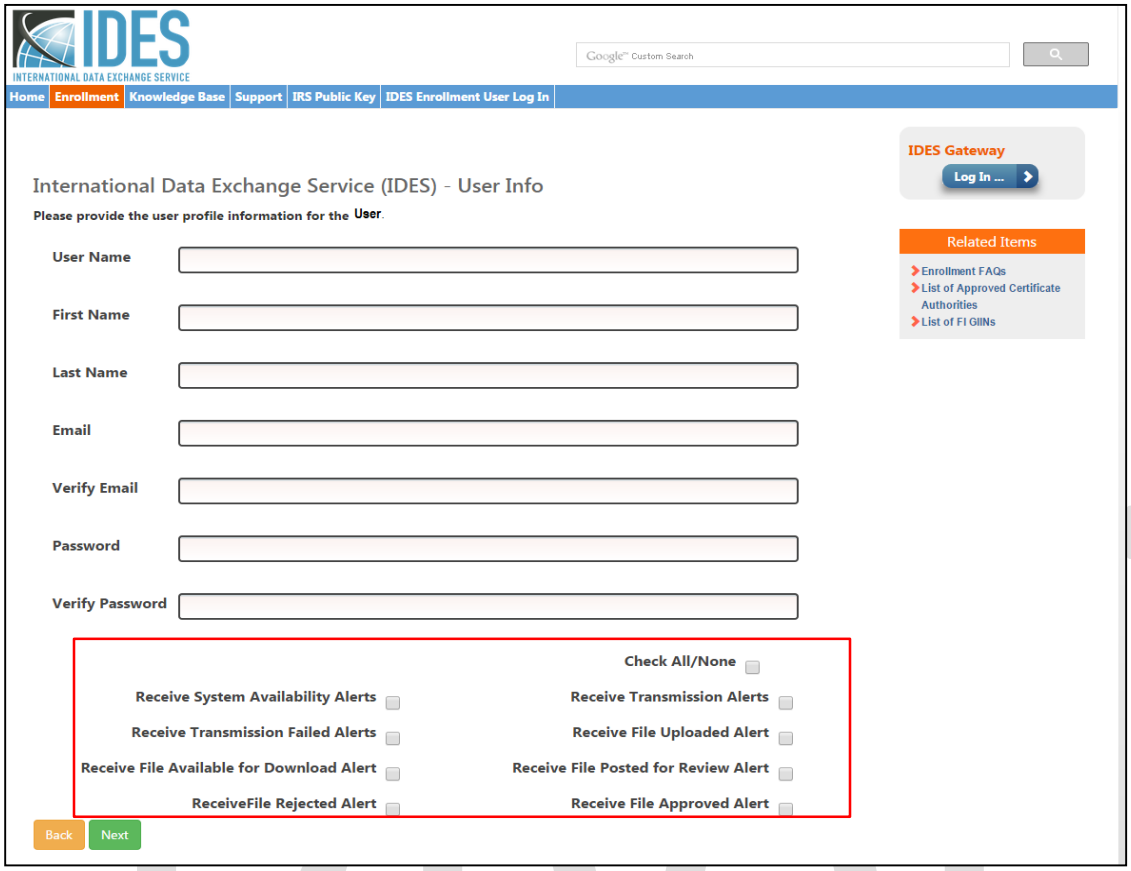


Figure 17

1. **Select Alert Preferences** – Click on the box next to the alerts you wish to receive by email. You can click the **Check All/None** box to choose all alerts or to remove all alerts. There are eight Alert Preferences
   a. **Receive System Availability Alerts** – IDES Enrollment and/or IDES Gateway are unavailable.
   b. **Receive Transmission Failed Alert** – transmission uploaded via the IDES Gateway failed for one of several reasons (e.g., virus, encryption validation, naming convention, package content). The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission failed.
   c. **Receive File Available for Download Alert** – the user has a file to download on the IDES Gateway. This is not functional at this time.
   d. **Receive File Rejected Alert** (for Model 1 Option 2 countries) – transmission upload was rejected by the HCTA. The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission was rejected.
   e. **Receive Transmission Alerts** – receive all IDES Alerts (See Alerts **b,c,d,f,g,h**).
   f. **Receive File Uploaded Alert** – received transmission is uploaded to the IRS for review.
   g. **Receive File Posted for Review Alert** (for Model 1 Option 2 countries) – sent to the HCTA when an FI uploads a report.
   h. **Receive File Approved Alert** (for Model 1 Option 2 countries) – sent after HCTA has approved the FI file.
2. Click **Next** to continue to upload digital certificate.

DRAFT

Upload Digital Certificate

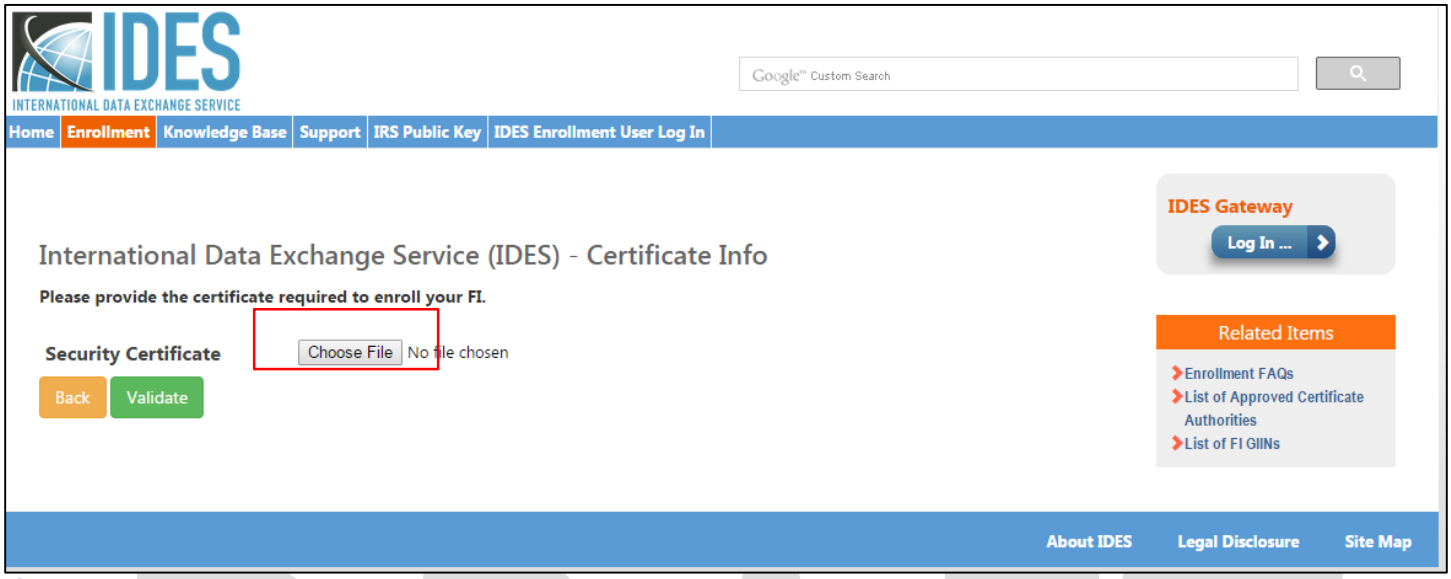


Figure 18

1. Click **Choose File** to search for the certificate located on your computer.

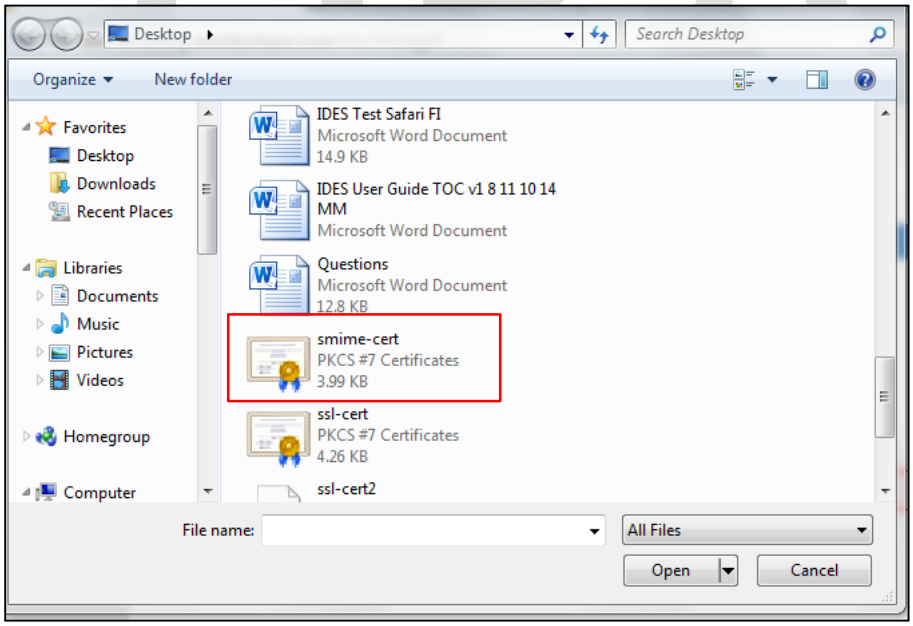


Figure 19

2. Select the Active/Valid certificate file from your computer.
3. Click **Open.**
4. Click **Validate.**
    a. If you receive an error message, refer to Appendix C: Certificate Upload Error Messages or contact IDES customer support for assistance.

DRAFT

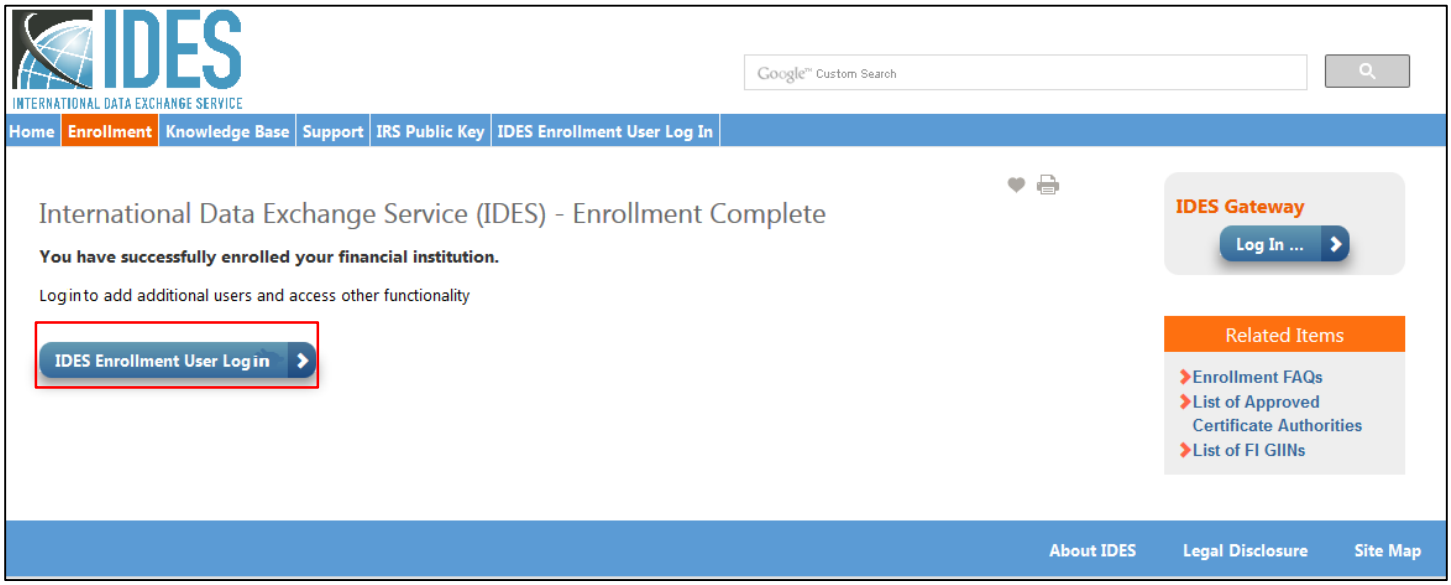


Figure 20

5. After you have validated your certificate, the enrollment process is complete. You will receive an email from the IDES help desk that verifies your authorization to access IDES Gateway.
6. Click **IDES Enrollment User Log In** to log in as the HCTA Administrator.

DRAFT

6. FI Administrators

Overview

Only registered FIs that have a valid GIIN may create an IDES account. The first user that registers for an IDES account, on behalf of their FI, is considered the Administrator. The FI Administrator is able to add, disable and enable end users, update the certificate, update alert preferences, create a metadata file, reset passwords, and download the IRS Public Key.

Financial Institutions include, but are not limited to:

- Depository institutions (for example, banks).
- Custodial institutions (for example, mutual funds).
- Investment entities (for example, hedge funds or private equity funds).
- Certain types of insurance companies that have cash value products or annuities.

End users (users under the FI Administrator) will be able to update their alert preferences, create a metadata file, and reset their password. To create an account, the FI Administrator will create challenge questions and a password. The FI Administrator will also upload the digital certificate received from an IRS approved Certificate Authority.

DRAFT

Begin Enrollment

The IDES enrollment site can be accessed at https://www.ides-support.com.

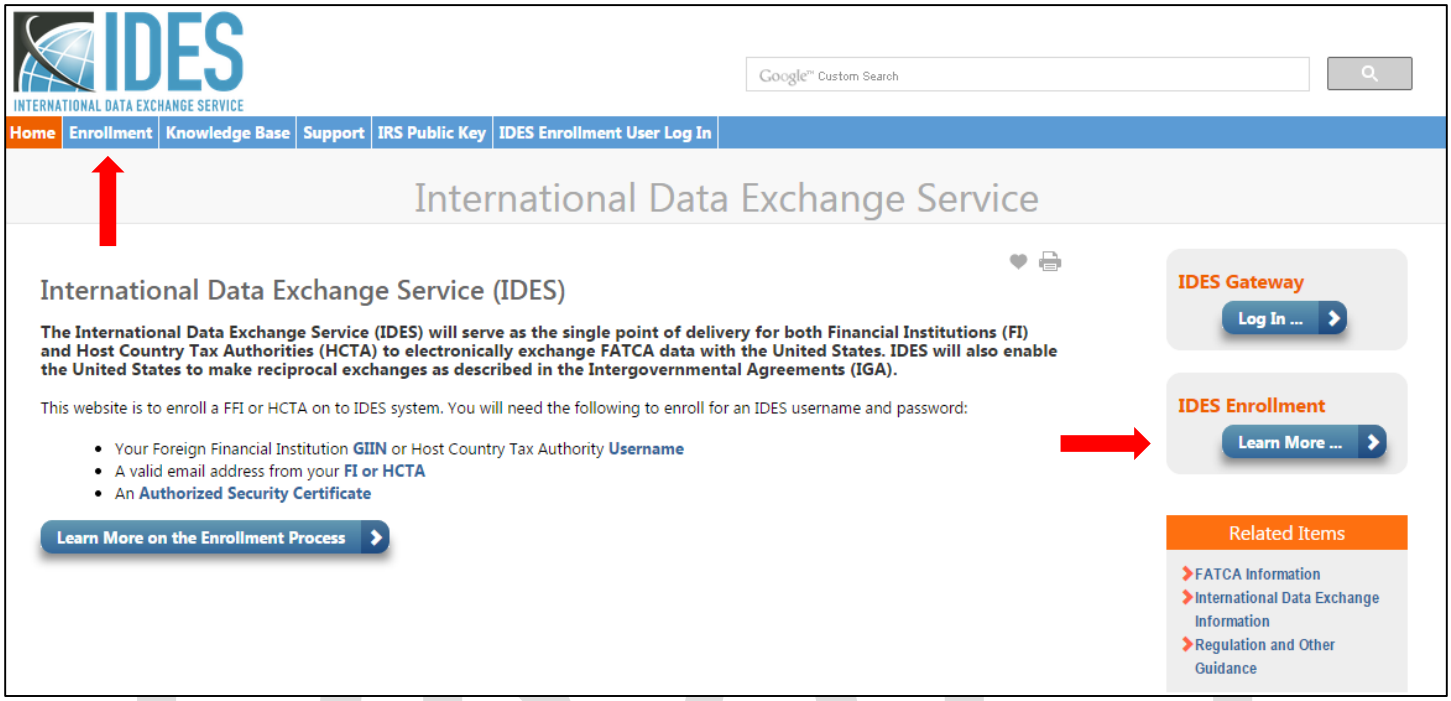


Figure 21

1. Click **Learn More** under IDES Enrollment or select the **Enrollment** tab.

DRAFT

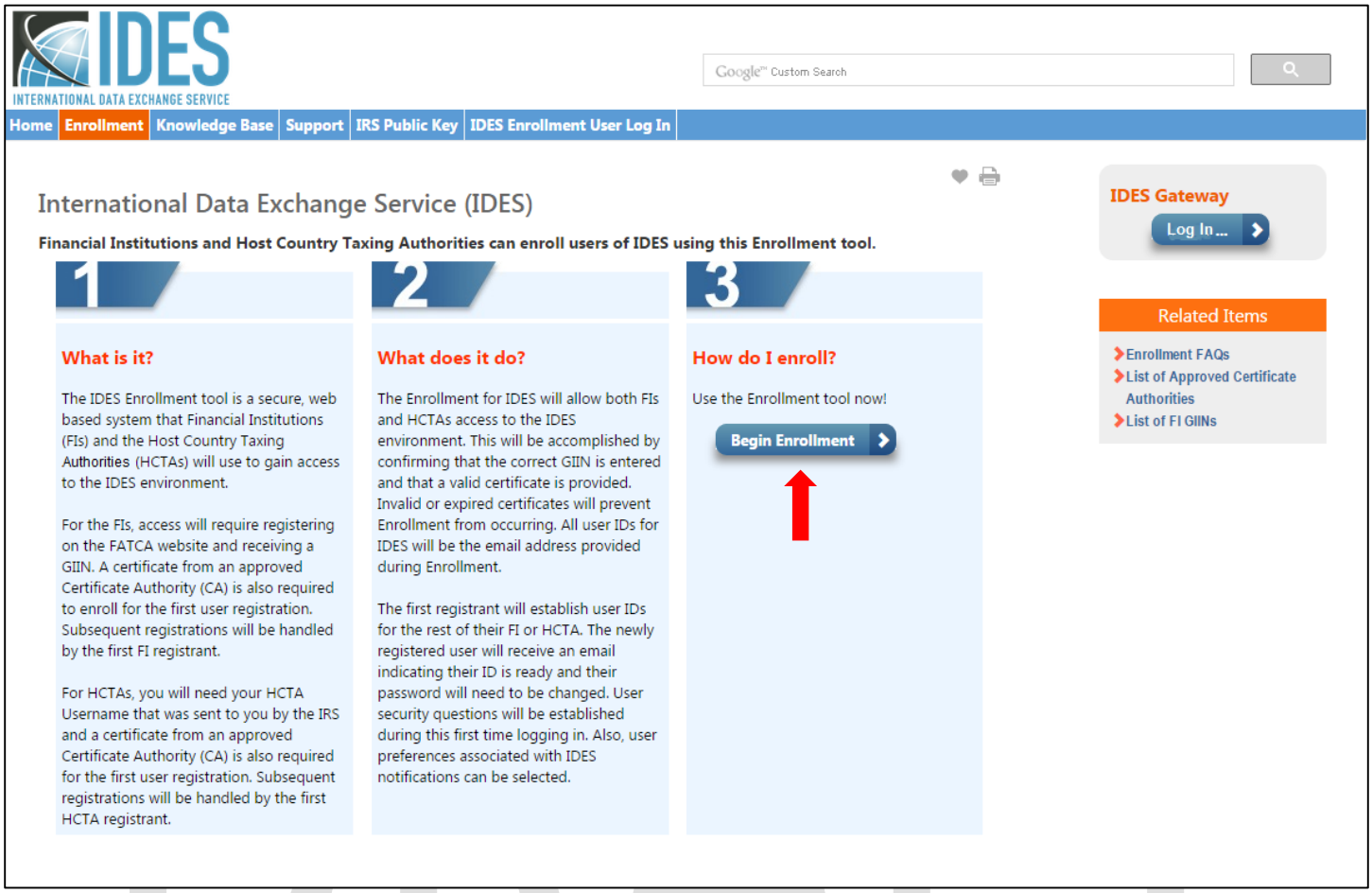


Figure 22

2. Click **Begin Enrollment** to start the enrollment process as an FI Administrator.

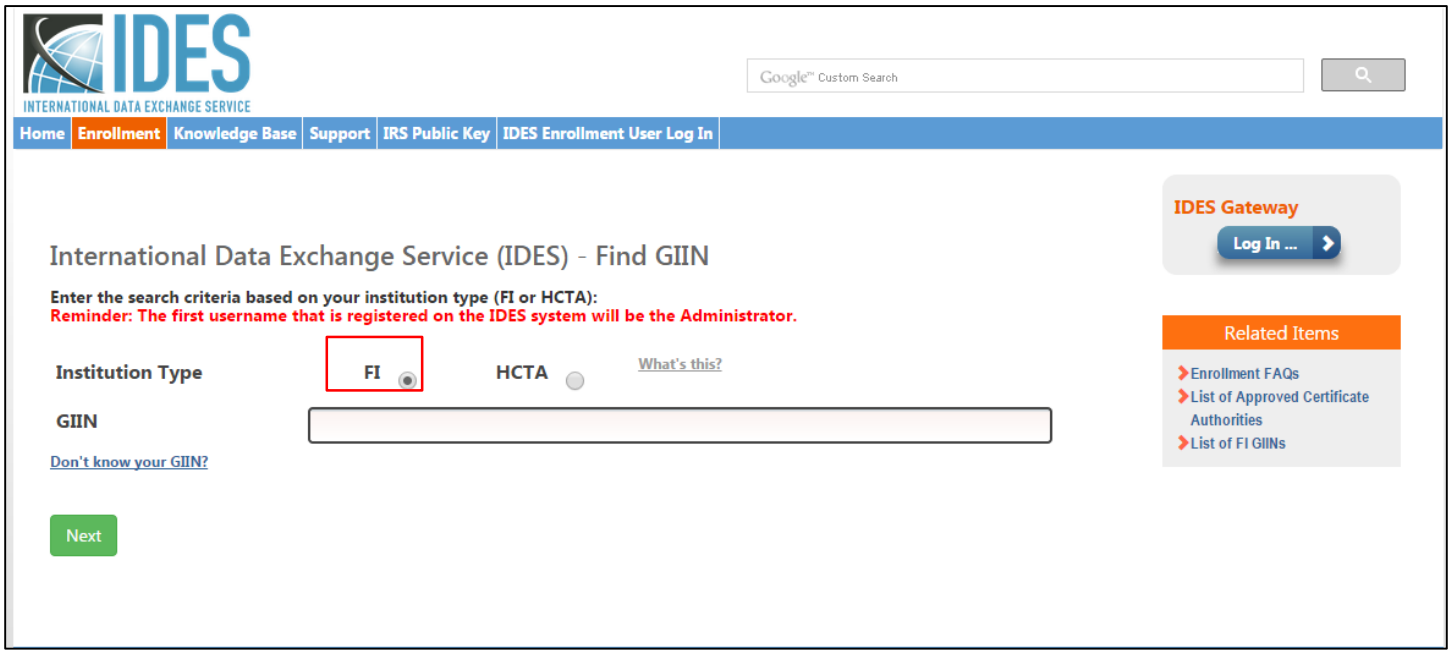


Figure 23

3. Select **Institution Type**, click **FI**.
4. **GIIN** – Enter the FI's GIIN in the 19-character format XXXXXX.XXXXX.XX.XXX.
5. Click **Next**.

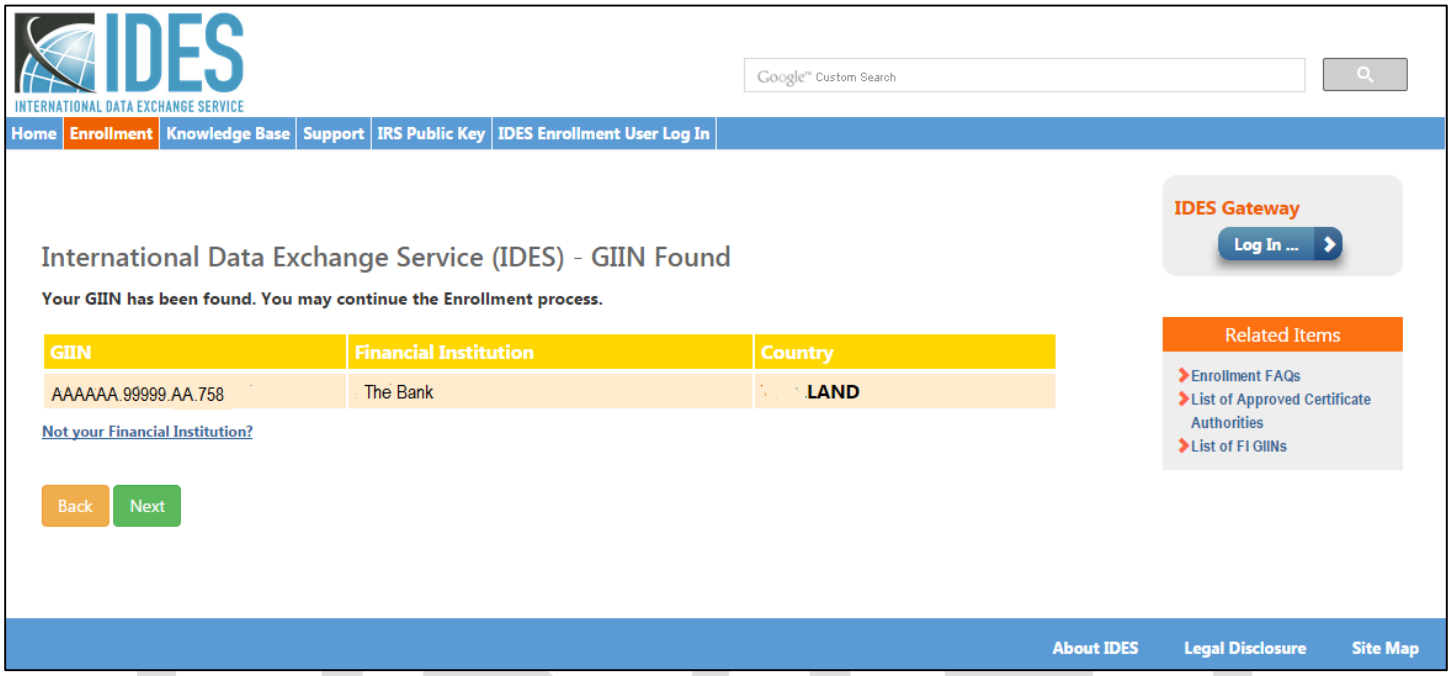


Figure 24

6. Confirm information and verify the **GIIN**, **Financial Institution** and **Country** are correct.
7. Click **Next** to continue and set up **Challenge Questions**.

DRAFT

Create Challenge Questions

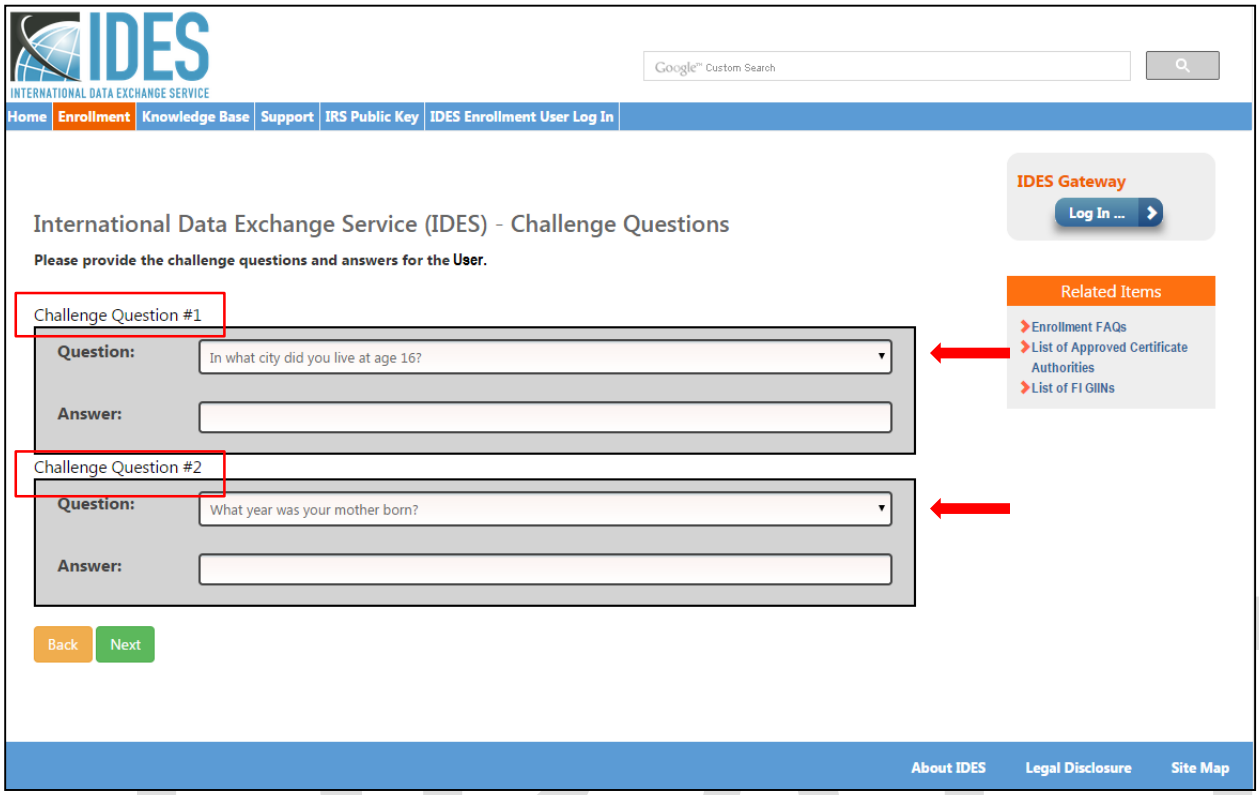


Figure 25

1. **Challenge Question #1**
    a. **Question:** Select the drop-down arrow to view a list of questions. Select a challenge question.
    b. **Answer:** Type a response to the challenge question.
2. **Challenge Question #2**
    a. **Question:** Select the drop-down arrow to view a list of questions. Select a challenge question.
    b. **Answer:** Type a response to the challenge question.
3. Click **Next** to continue and set up a **Username**.

IMPORTANT: Remember to document answers to the challenge questions. Users may need these to reset a password or to contact the IDES Help Desk.

DRAFT

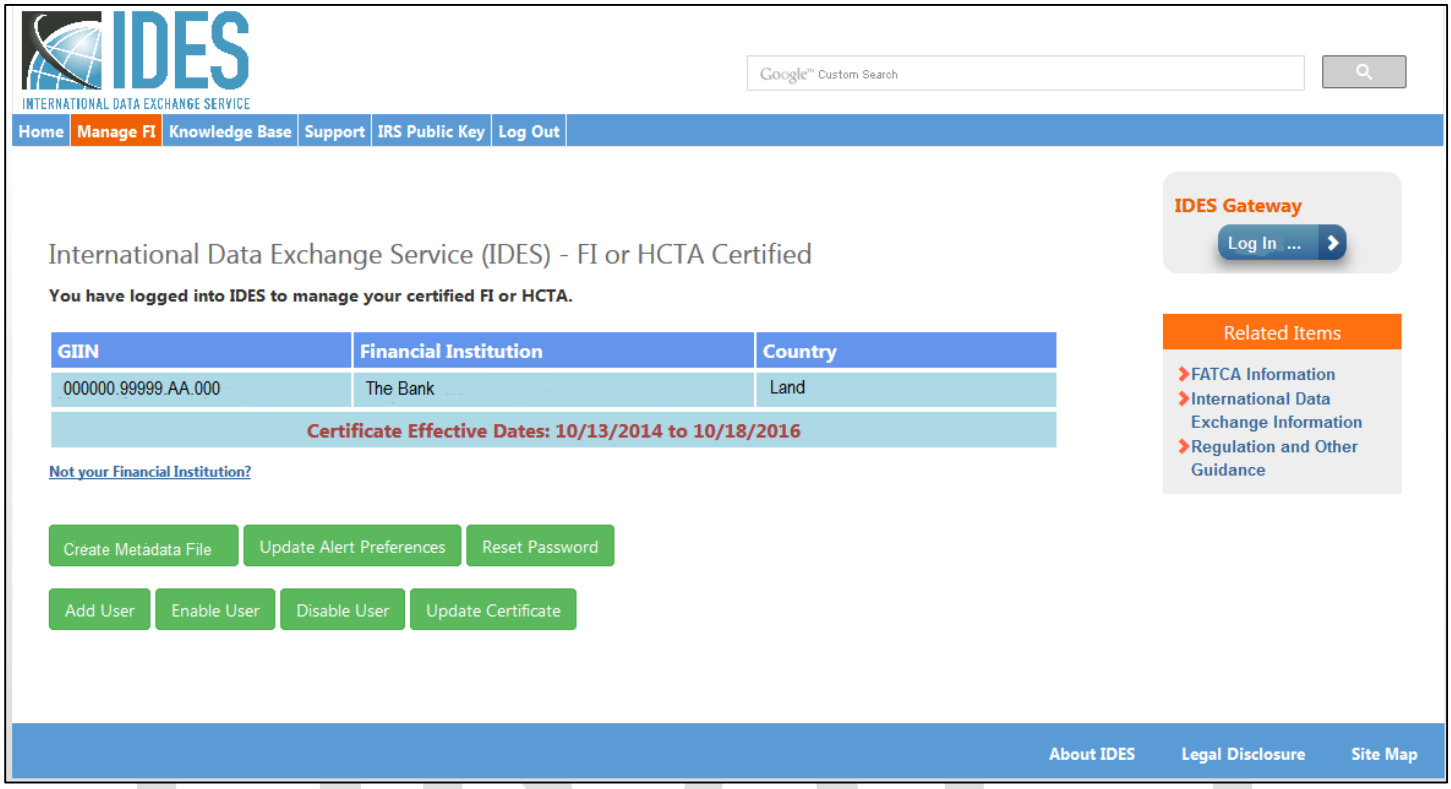


Figure 26

DRAFT

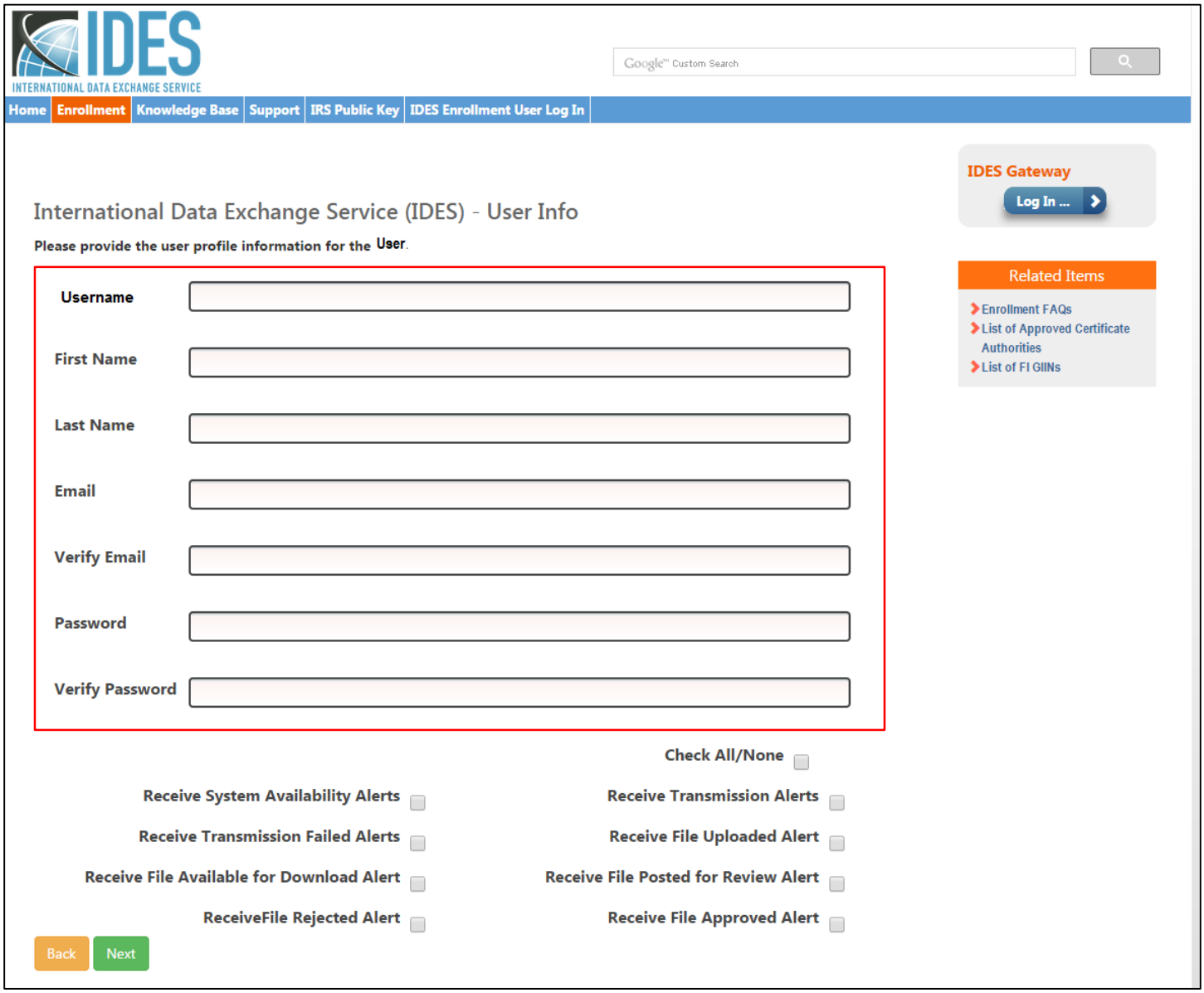


Figure 27

1. **Username** – Enter your new username. We recommend first initial and last name. If the username is already taken you will receive an error message.
2. **First Name** – Enter your first name.
3. **Last Name** – Enter your last name.
4. **Email** – Enter your email address.
5. **Verify Email** – Enter your email address again (must match the previous entry). If it does not match, you will receive an error message.
6. **Password** – Create a valid password.
    a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .).
    b. If you enter a password that does not meet the guidelines, you will receive an error message.
7. **Verify Password** – Re-type your password (must match the previous entry). If it does not match, you will receive an error message.

Select Alert Preferences

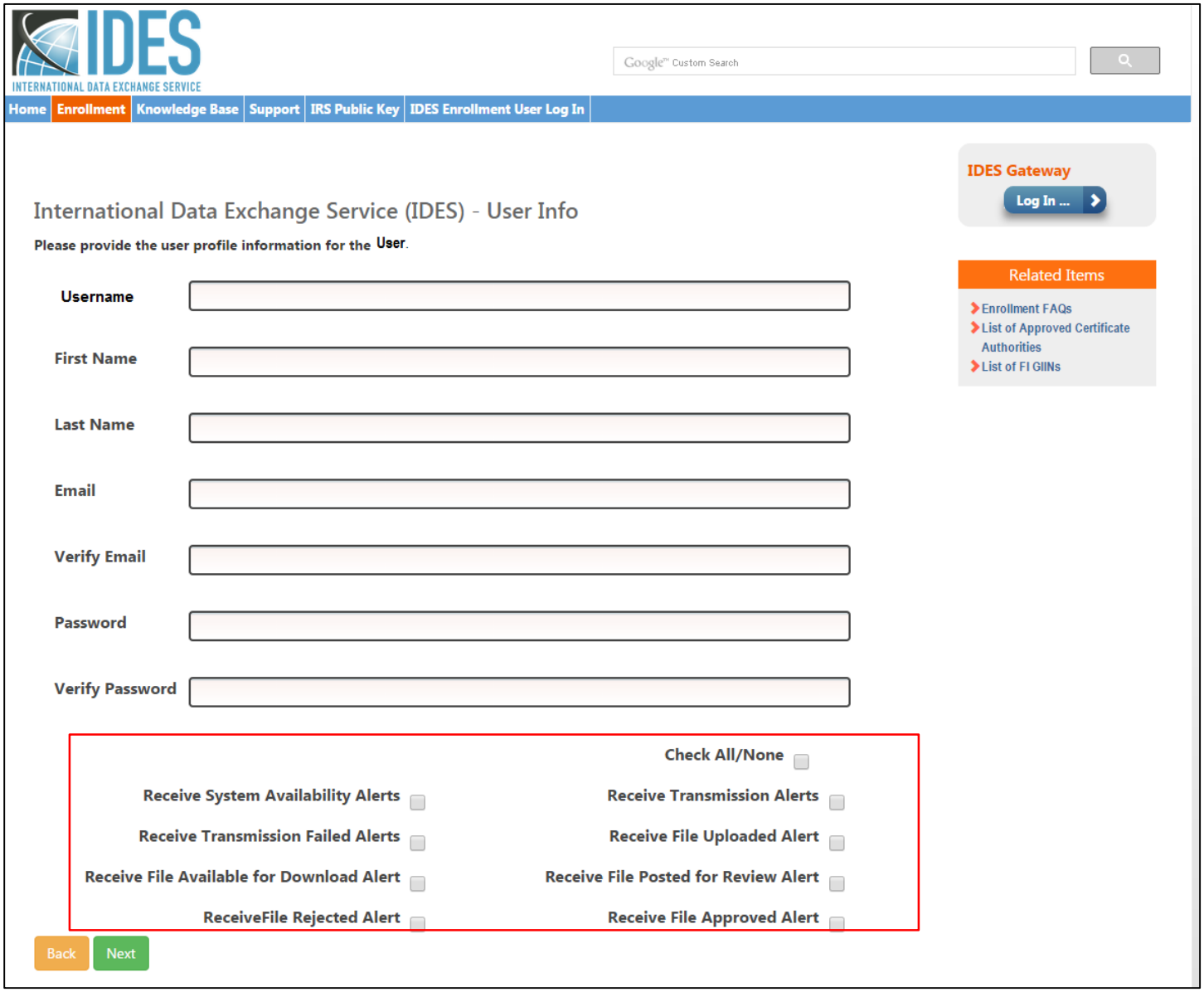


Figure 28

1. **Select Alert Preferences** – Click on the box next to the alerts you wish to receive by email. You can click the **Check All/None** box to choose all alerts or to remove all alerts. There are eight Alert Preferences
   a. **Receive System Availability Alerts** – IDES Enrollment and/or IDES Gateway are unavailable.
   b. **Receive Transmission Failed Alert** – transmission uploaded via the IDES Gateway failed for one of several reasons (e.g., virus, encryption validation, naming convention, package content). The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission failed.
   c. **Receive File Available for Download Alert** – the user has a file to download on the IDES Gateway. This is not functional at this time.
   d. **Receive File Rejected Alert** (for Model 1 Option 2 countries) – transmission upload was rejected by the HCTA. The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission was rejected.

e. **Receive Transmission Alerts** – Receive all IDES Alerts (See Alerts **b,c,d,f,g,h**).
f. **Receive File Uploaded Alert** – received transmission is uploaded to the IRS for review.
g. **Receive File Posted for Review Alert** (for Model 1 Option 2 countries) – sent to the HCTA when an FI uploads a report.
h. **Receive File Approved Alert** (for Model 1 Option 2 countries) – sent after HCTA has approved the FI file.

2. Click **Next** to continue to upload digital certificate.

Upload Digital Certificate

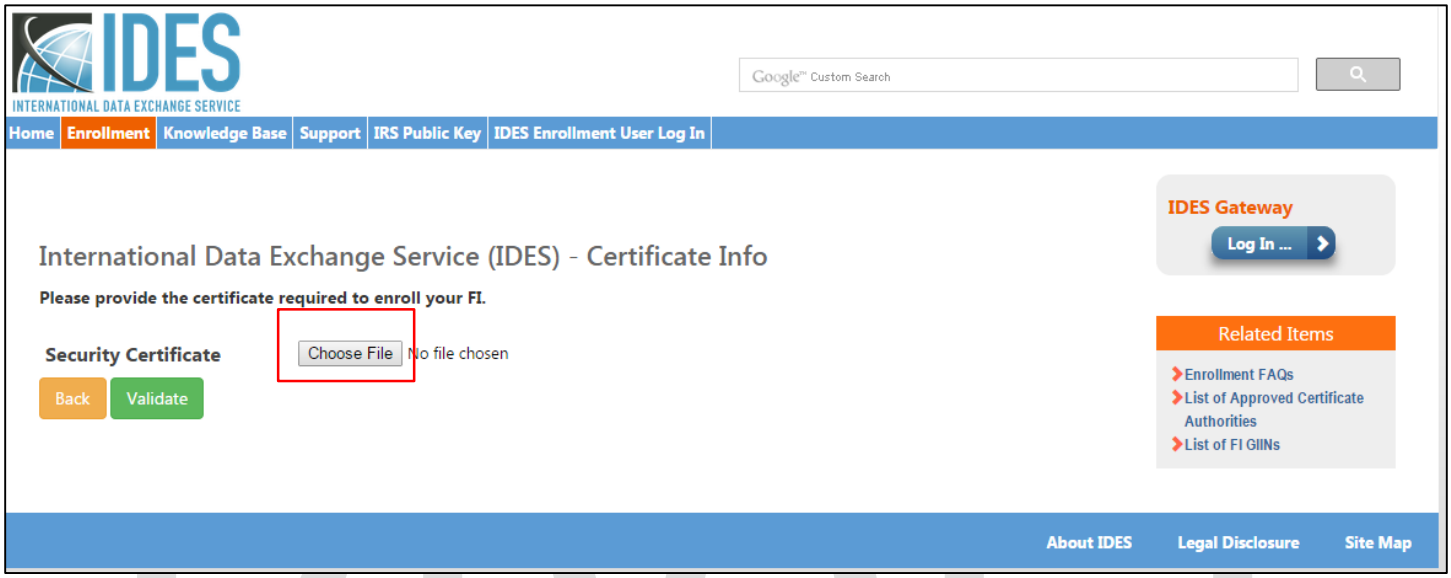


Figure 29

1. Click **Choose File** to search for the security certificate located on computer.

DRAFT

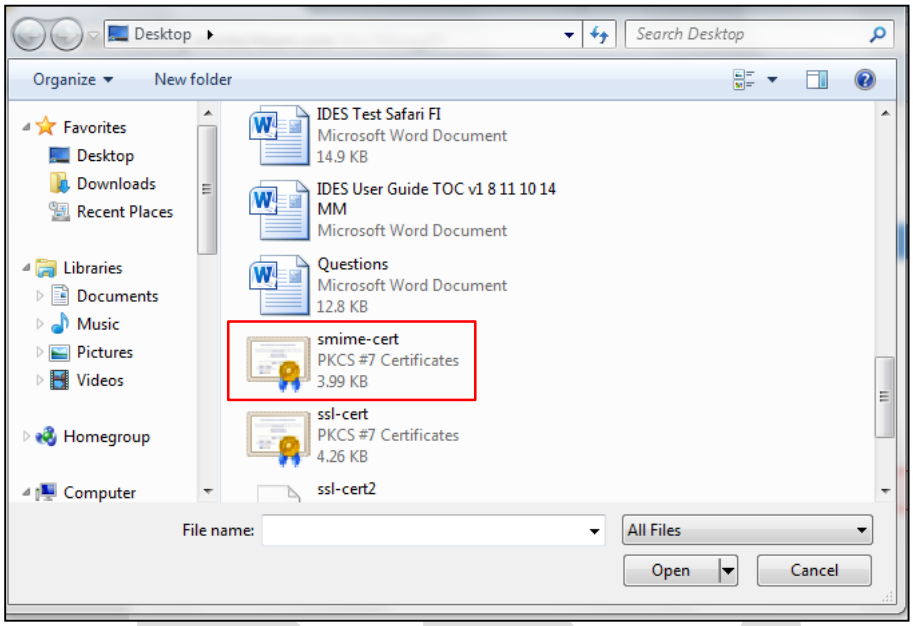


Figure 30

2. Select the Active/Valid certificate file from your computer.
3. Click **Open.**
4. Click **Validate.**
    a. If you receive an error message, refer to Appendix C: Certificate Upload Error Messages or contact IDES customer support for assistance.

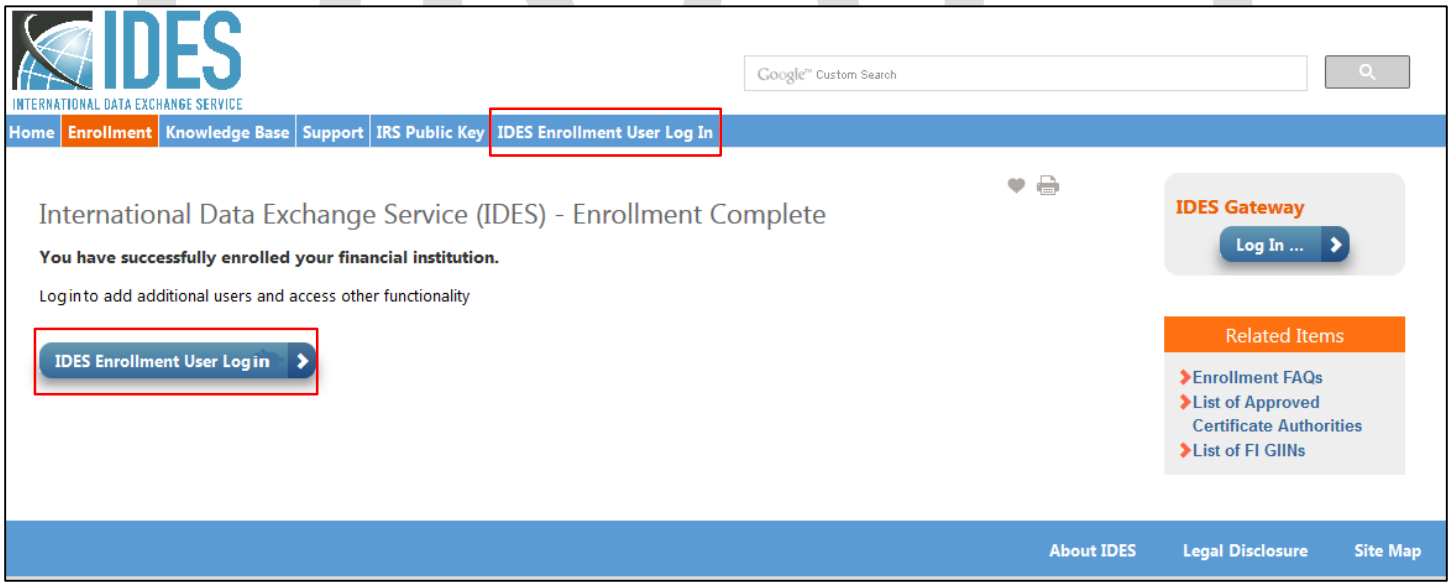


Figure 31

5. After you have validated your certificate, the enrollment process is complete. You will receive an email from the IDES help desk that verifies your authorization to access IDES Gateway.
6. Click **IDES Enrollment User Log In** to log in as the FI Administrator.

DRAFT

7. Existing Administrators (HCTA and FI)

HCTA and FI Administrators can add end users, disable and enable end users, update the certificate, update alert preferences, create a metadata file, reset passwords, and download an IRS public key.

Add a User

End users added under FI and HCTA Administrator accounts are able to perform the following functions:

- Create a Metadata File.
- Update Alert Notifications.
- Reset Password.
- Download the IRS Public Key.

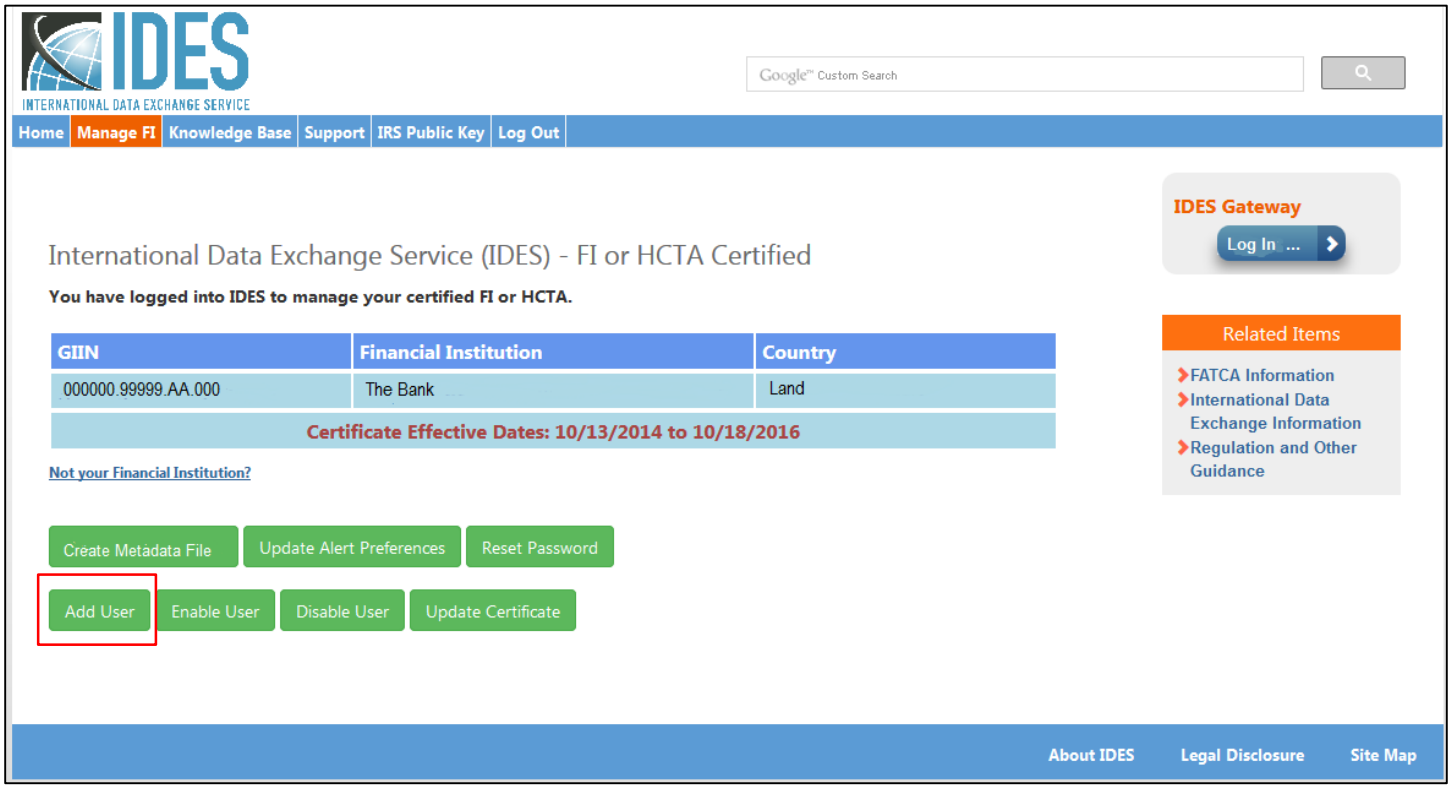


Figure 32

1. Click **Add User.**

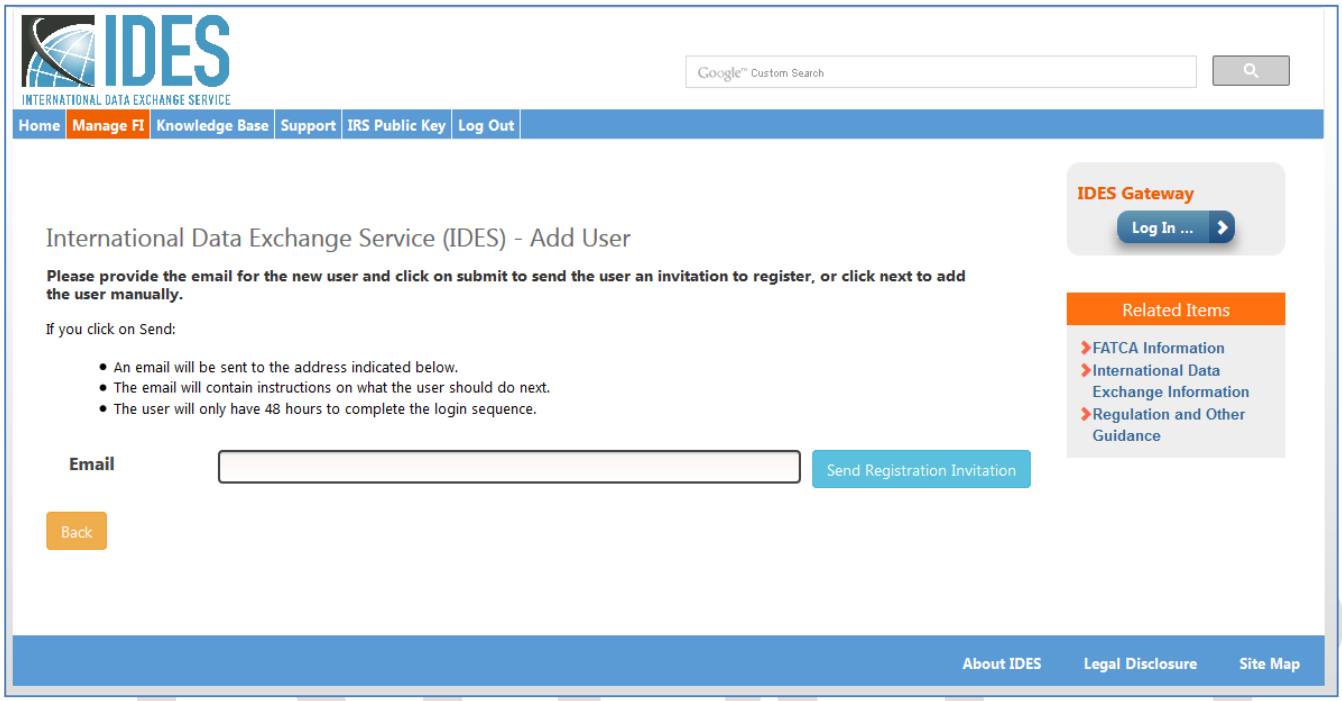


Figure 33

2. **Email** - Type in email address of new end user.
3. Click **Send Enrollment Invitation**.

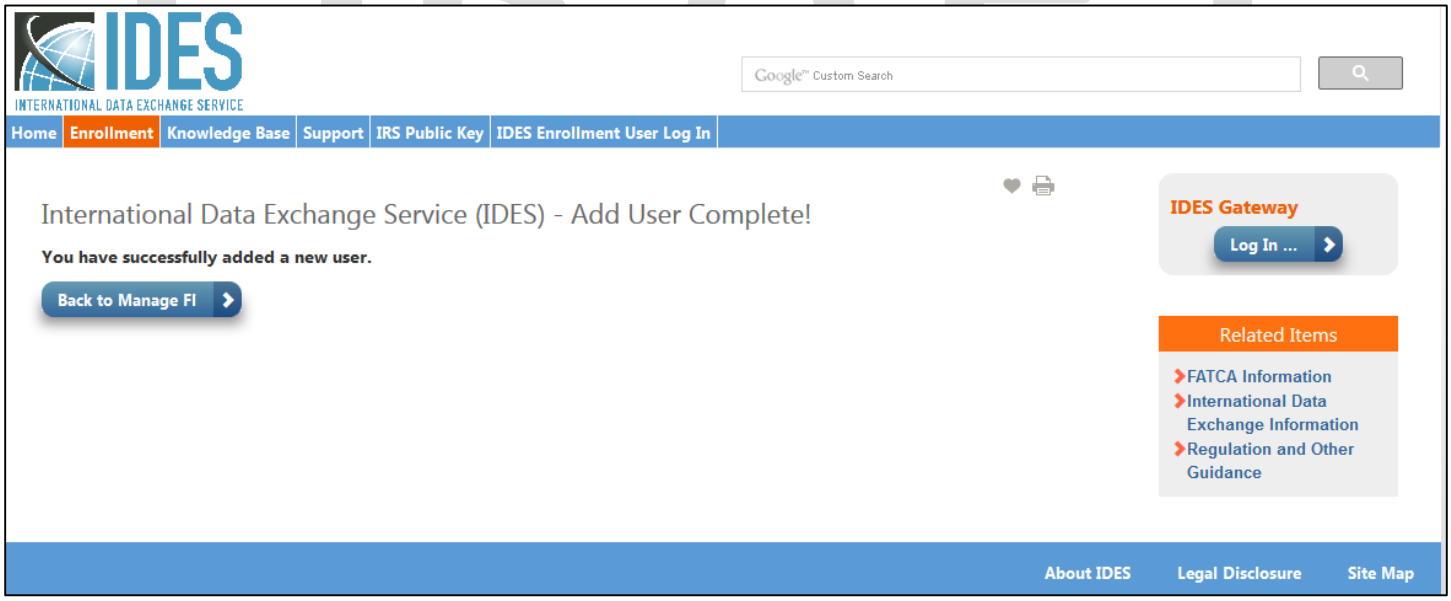


Figure 34

4. The new end user will receive an email to register. The link in the email is valid for 48 hours.
5. Confirmation of End User **Enrollment Invitation** email has been sent.

DRAFT

Welcome to International Data Exchange Service! Your corporate administrator has registered you as an authorized user.

To log in to International Data Exchange Service (IDES), complete the following steps:

1. Click on this link to enroll in IDES.
2. Create password challenge questions. Challenge questions will be used to prompt you if you forget your password. By correctly responding to the challenge questions, you can reset your password without contacting the IDES help desk.
3. Create your IDES user name and password.

SHARING USER IDs AND PASSWORDS IS NOT ALLOWED. If you have additional people who will use IDES, they must obtain their own user IDs. You are responsible for any activity associated with your user ID, so do not share your password with anyone, including the IDES help desk.

Need help?

If you need help using IDES or have questions about IDES policies, please contact IDES Customer Support by phone at 1-800-613-IDES (4773) or by email at helpdesk@ides-support.com. IDES Customer Support is available 24 hours a day except on U.S. federal holidays .

Additionally, the IDES team is always interested in improving our service. Please contact us through IDES Customer Support with suggestions on how to make IDES work better for you.

We are excited that you have joined IDES and we are committed to helping your organization.

Regards,
The IDES Team

Figure 35

6. The new end user will receive a copy of the above email. If the end user does not receive this email, contact IDES customer support for assistance.

Disable a User

Administrators can disable an end user at any time. Administrations are not authorized to delete accounts, but disabling will prevent all access to IDES. Administrators may enable this end user at a later date.

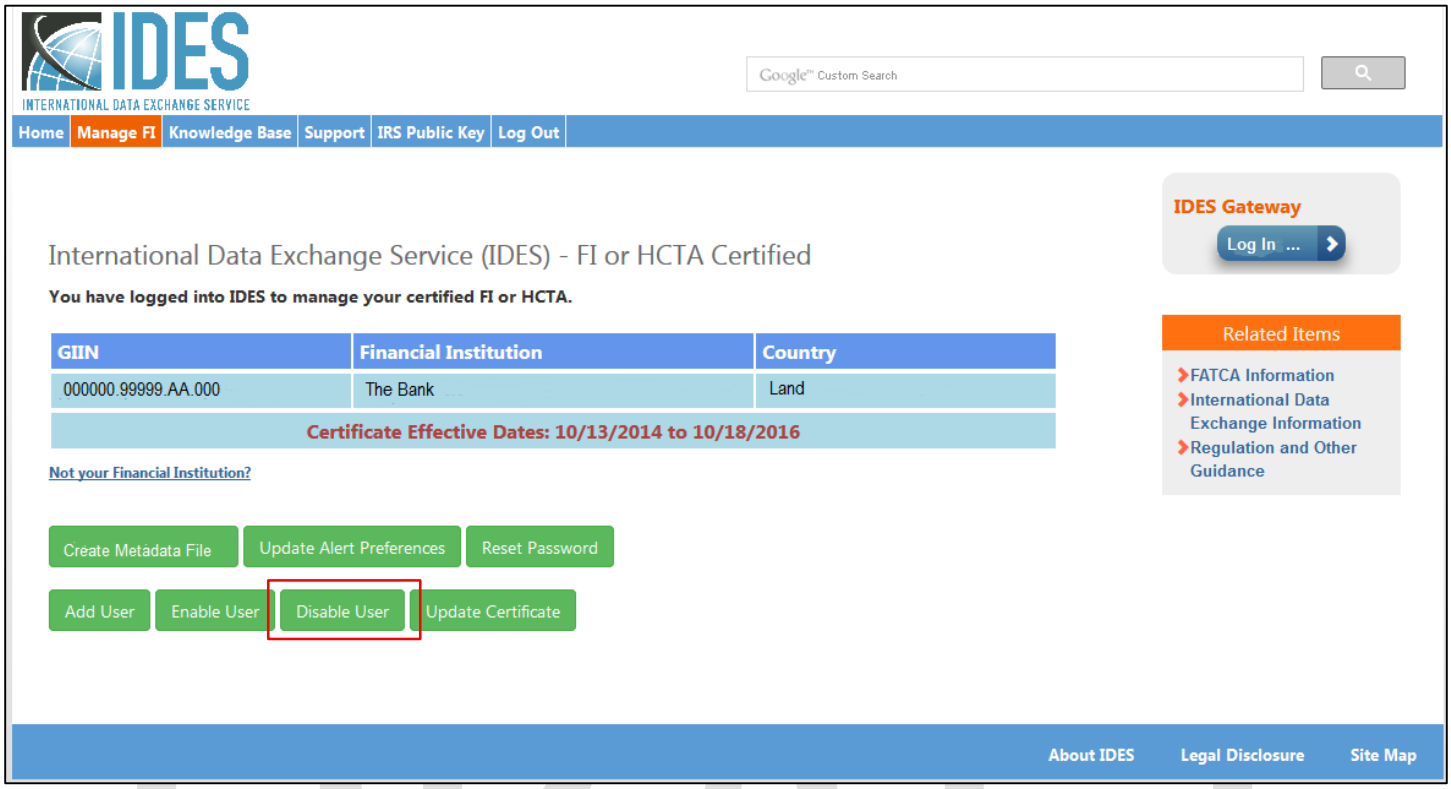


Figure 36

1. Click **Disable User**.

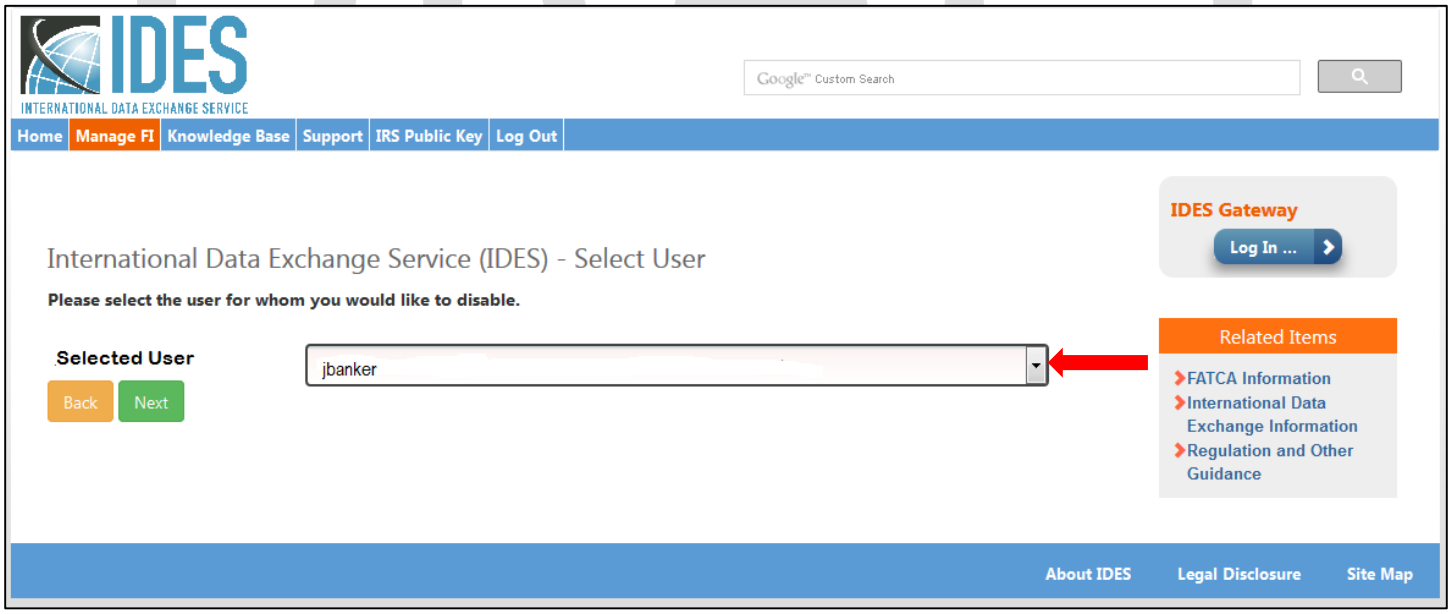


Figure 37

2. **Selected User** – Select the end user that you want to disable from the drop down box by clicking the arrow.
3. Click **Next**.

DRAFT

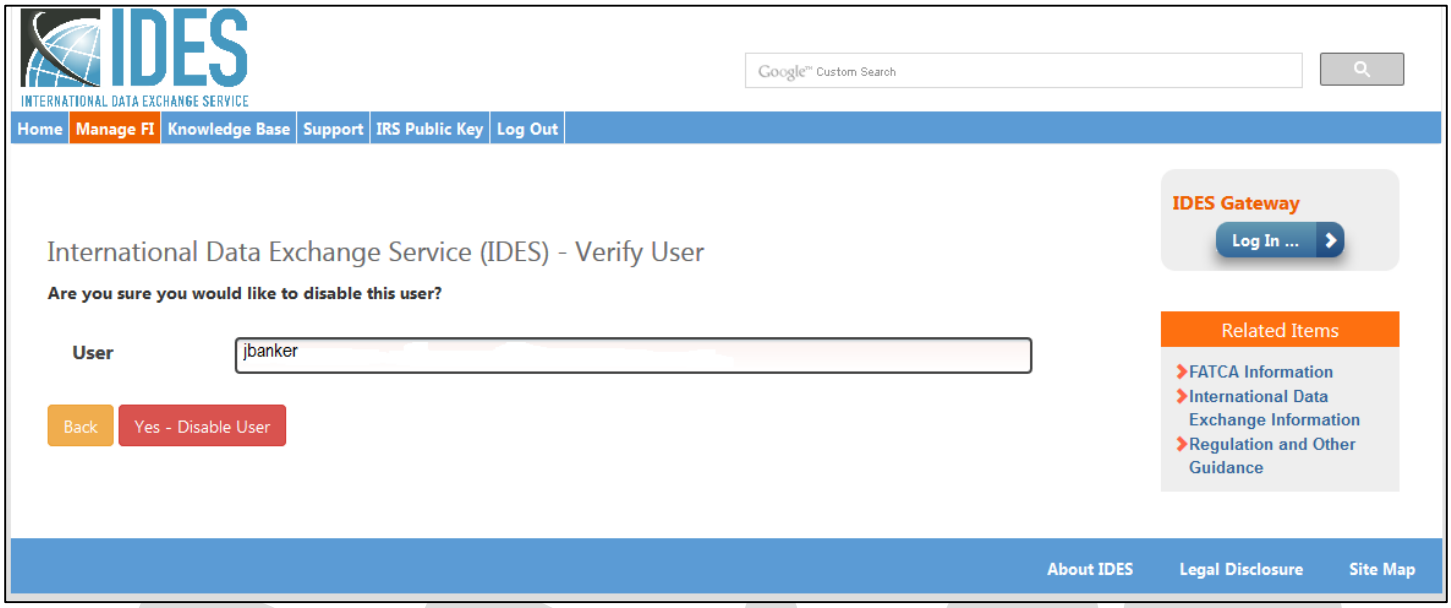


Figure 38

4. **User** – Verify that you have selected the correct username.
5. Click **Yes – Disable User**.

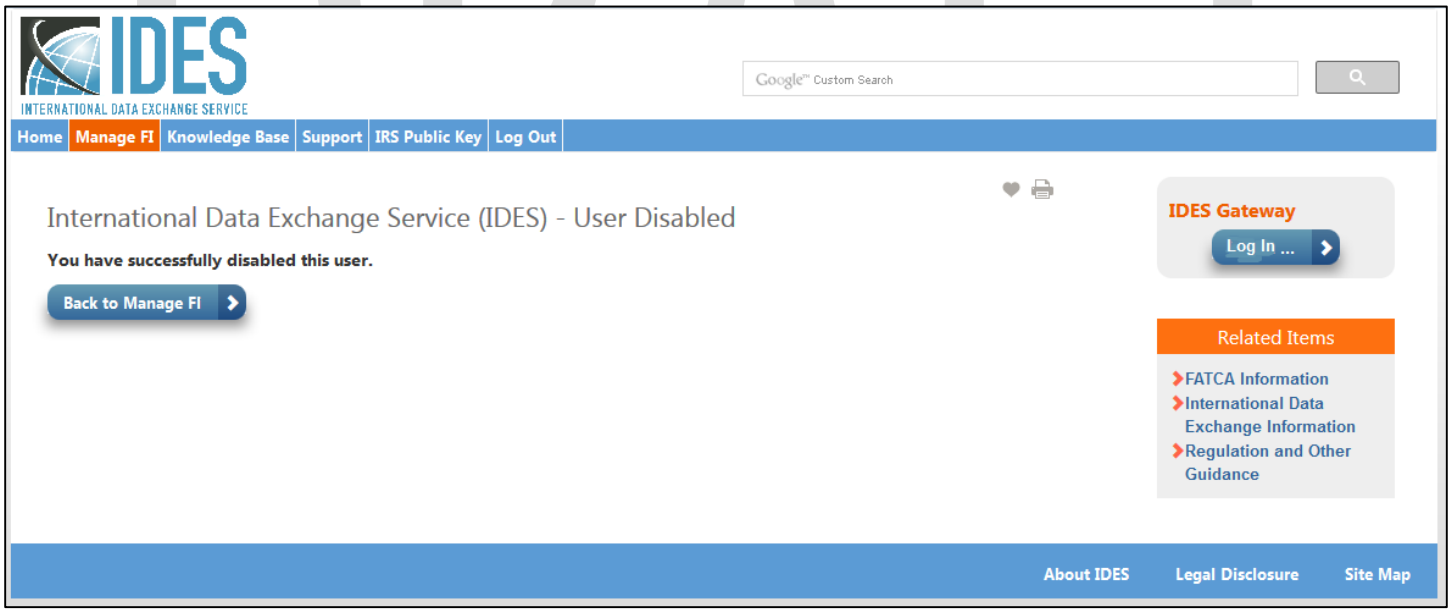


Figure 39

6. Receive confirmation that the end user has been disabled.

DRAFT

Enable a User

Administrators can only use the Enable User option to enable end users that were previously disabled. To add a new end user, administrators must follow the process for Add a User.

After the Administrator has enabled the end user, the account and previous password will be active again. If the end user does not remember his or her password, the Administrator can reset the password or the end user can follow the Forgot Password process.

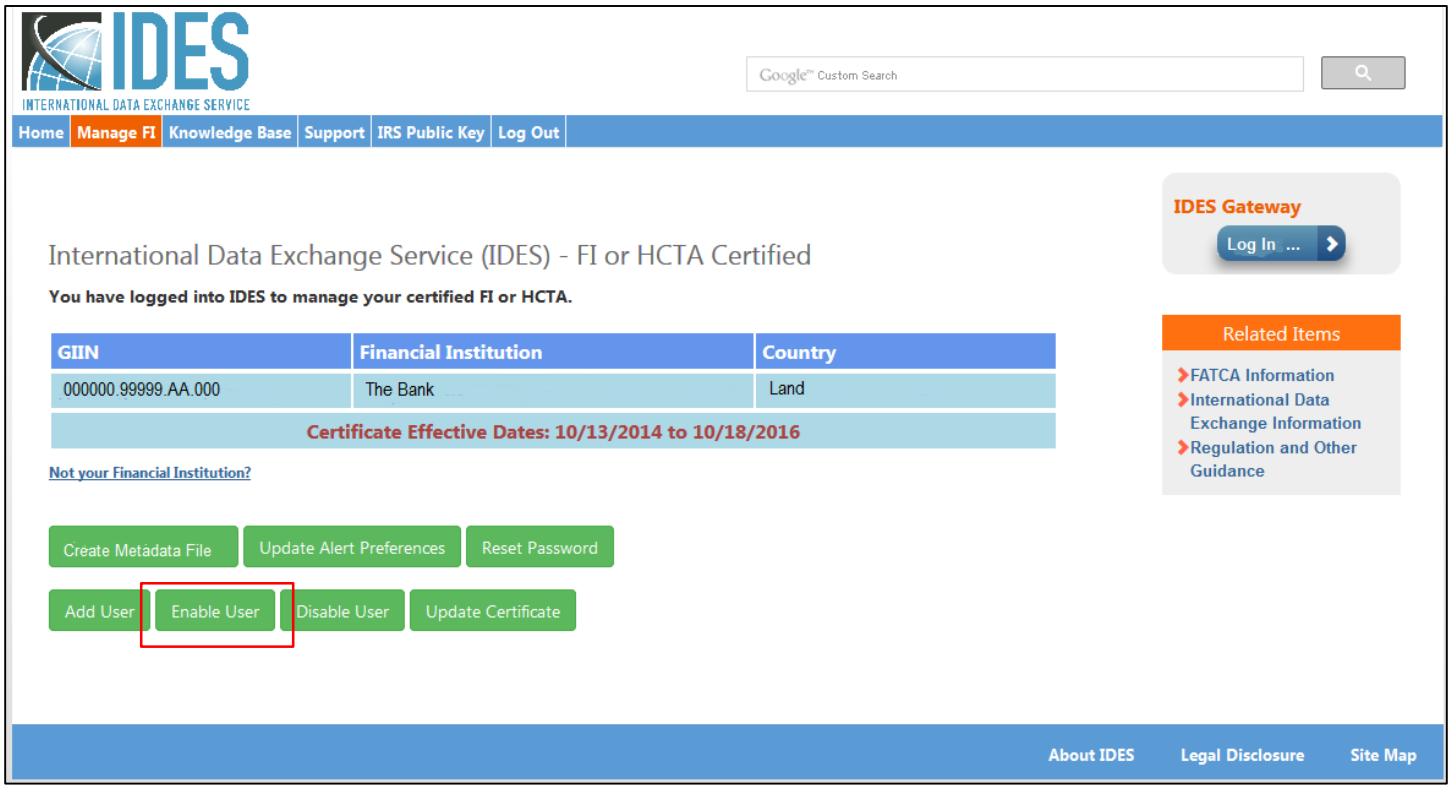


Figure 40

1. Click **Enable User.**

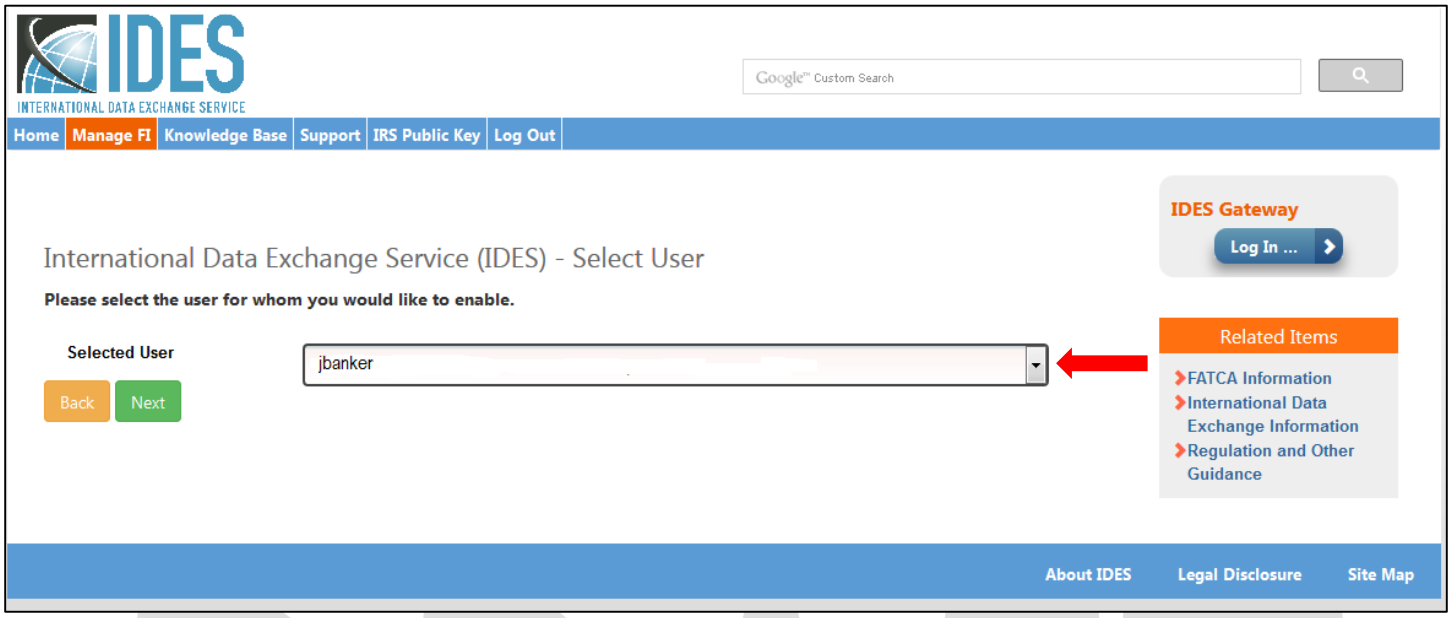


Figure 41

2. **Selected User** – Select the end user that you want to enable from the drop down box by clicking the arrow.
3. Click **Next** to confirm.

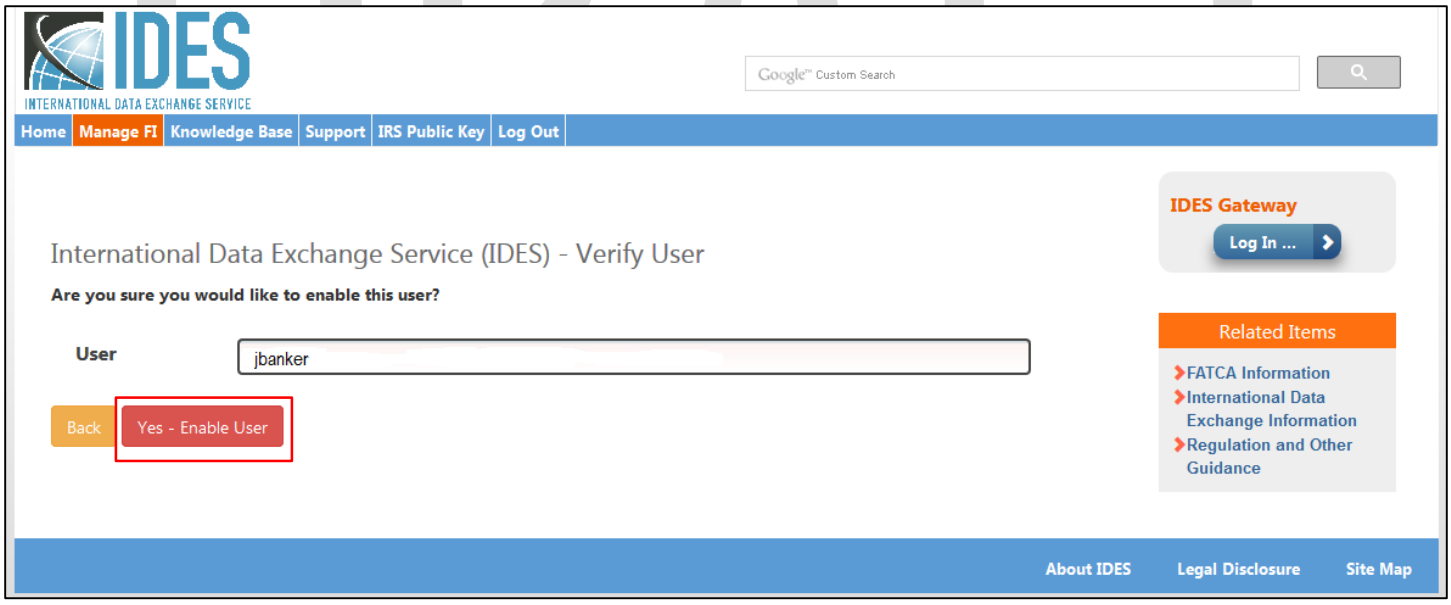


Figure 42

4. **User** – Verify the user to enable.
5. Click **Yes – Enable User**.

DRAFT

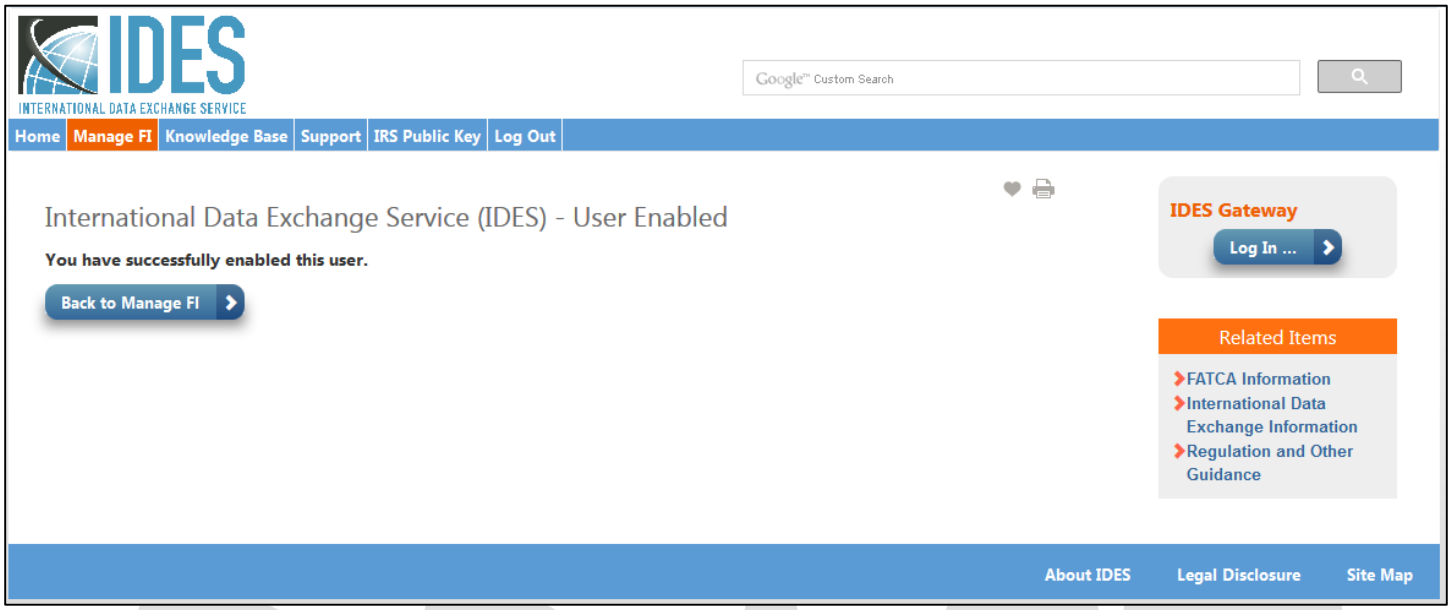


Figure 43

6. Receive confirmation that the end user has been enabled.

DRAFT

Update the Certificate

Administrators will need to update invalid or expired certificates.

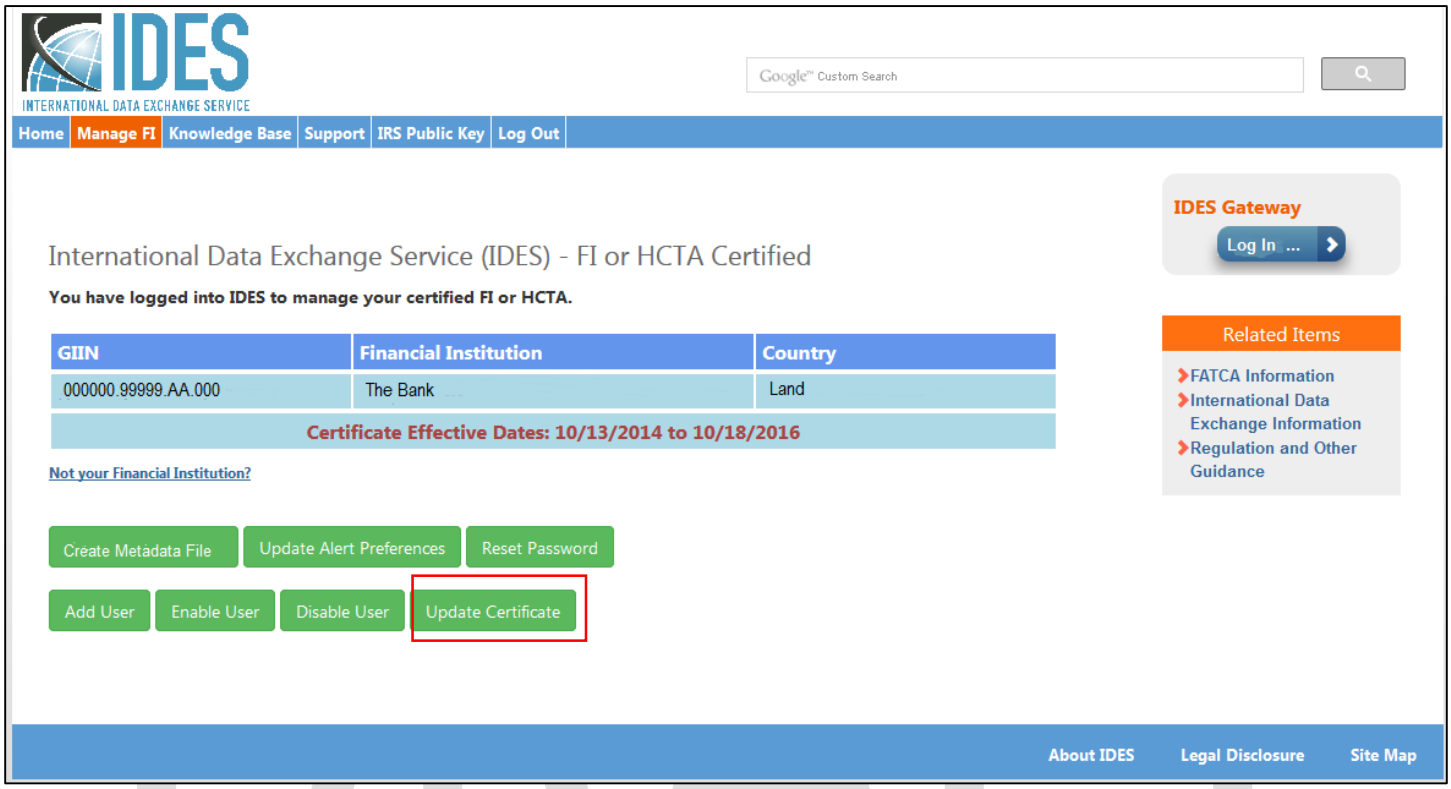


Figure 44

1. Click on **Update Certificate.**

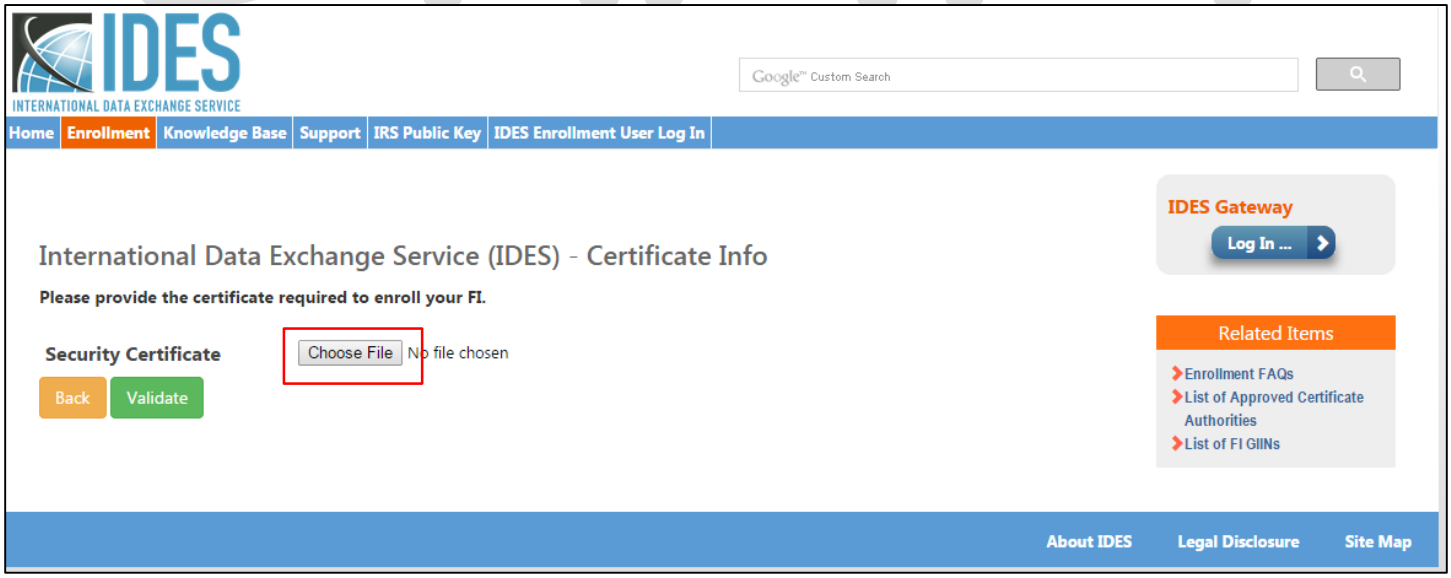


Figure 45

2. Click **Choose File** to upload the new certificate from your computer.

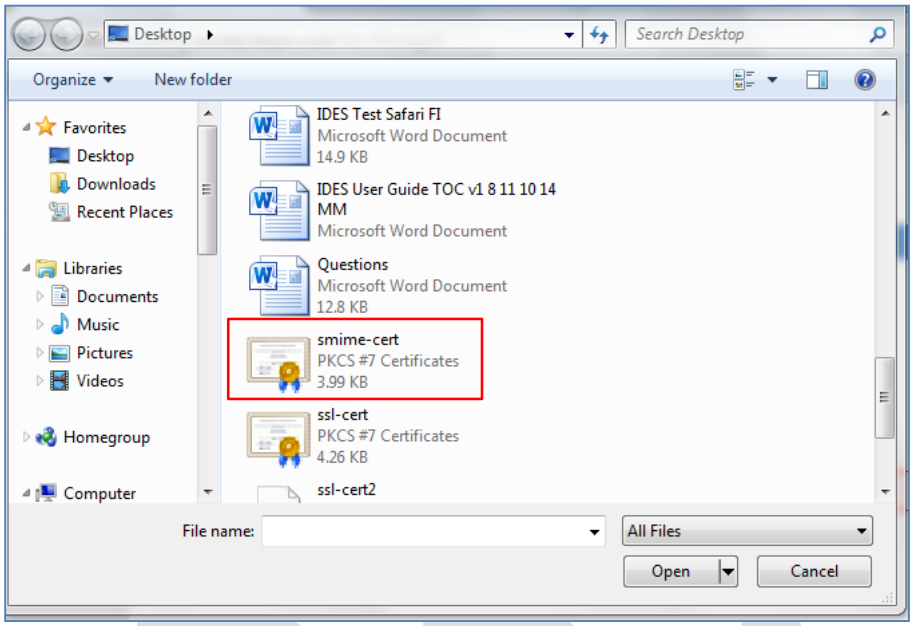


Figure 46

3. Click on the certificate file then click **Open** to load the file.

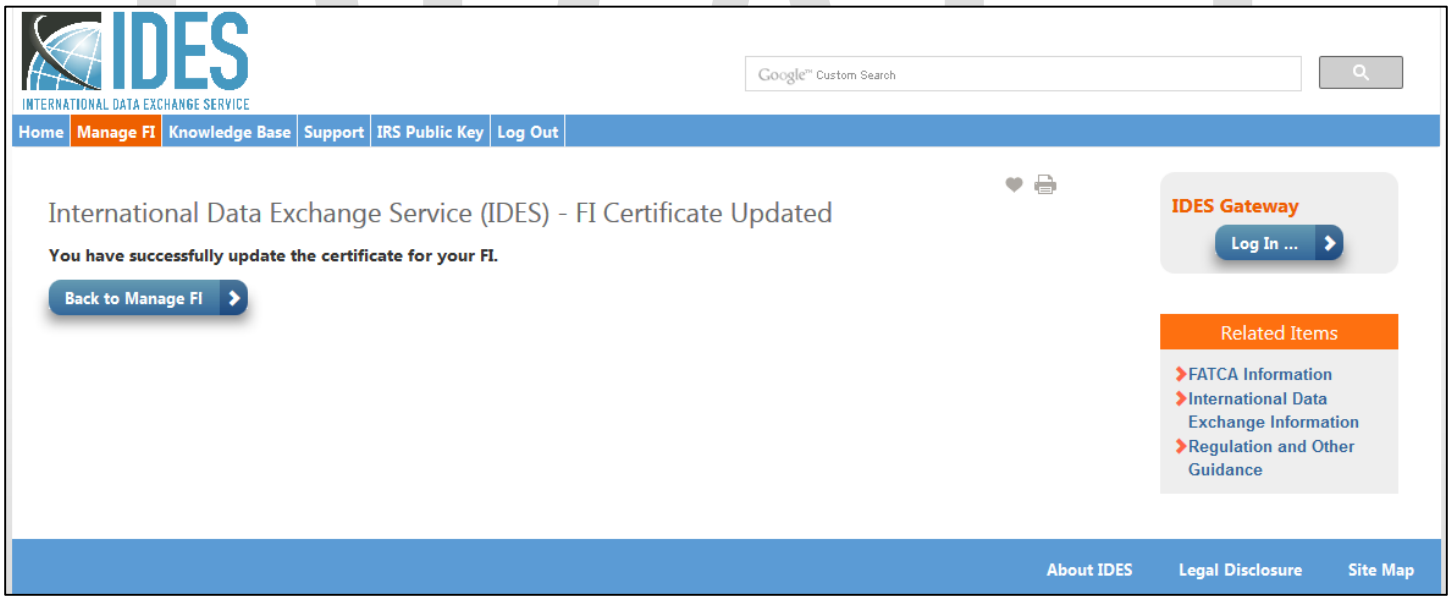


Figure 47

4. Click **Validate** to complete the upload of the new certificate. If you receive a certificate error message, refer to Appendix C: Certificate Upload Error Messages for a complete list or contact IDES customer support.
5. Review confirmation screen of successful certificate update.

DRAFT

Update Alert Preferences

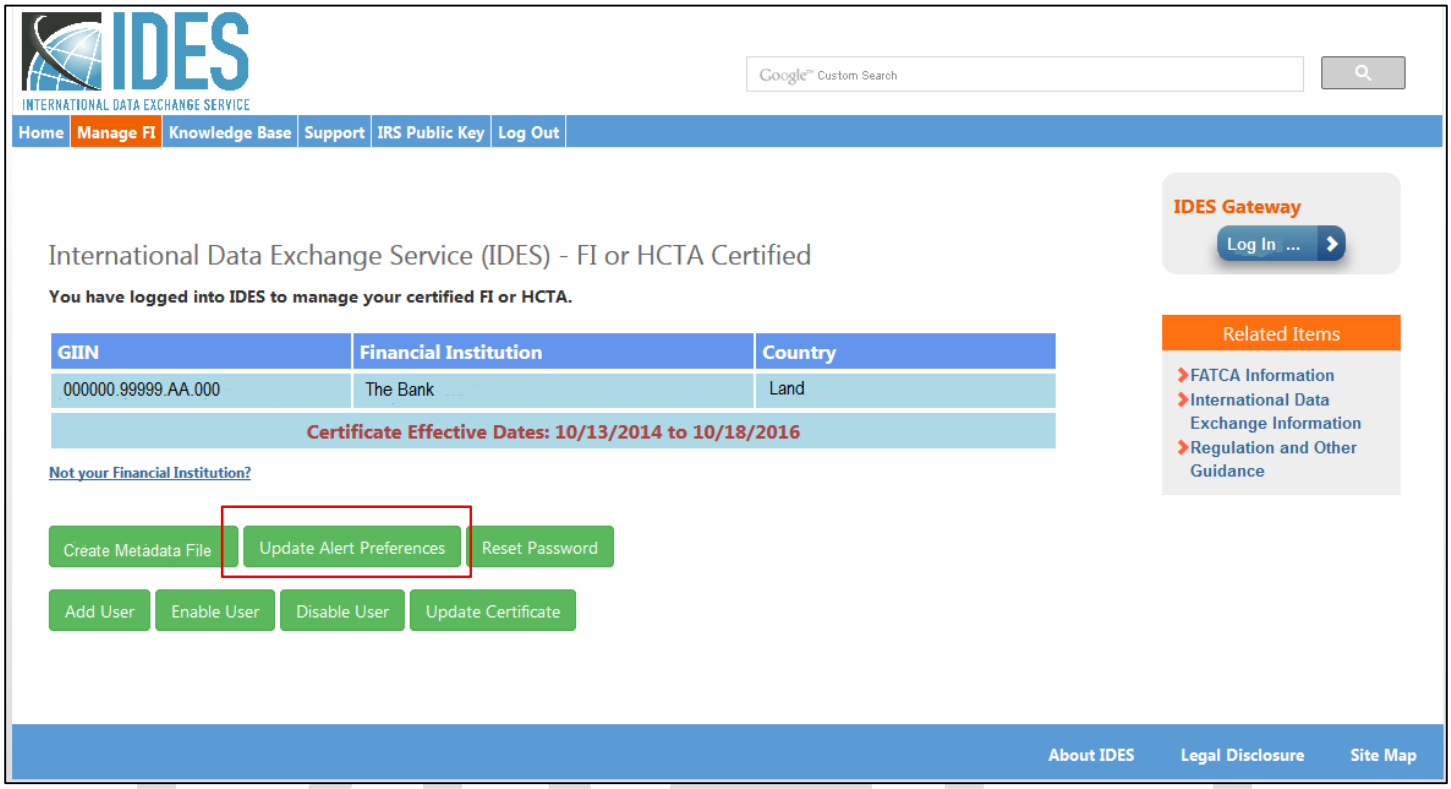


Figure 48

1. Click **Update Alert Preferences.**

DRAFT

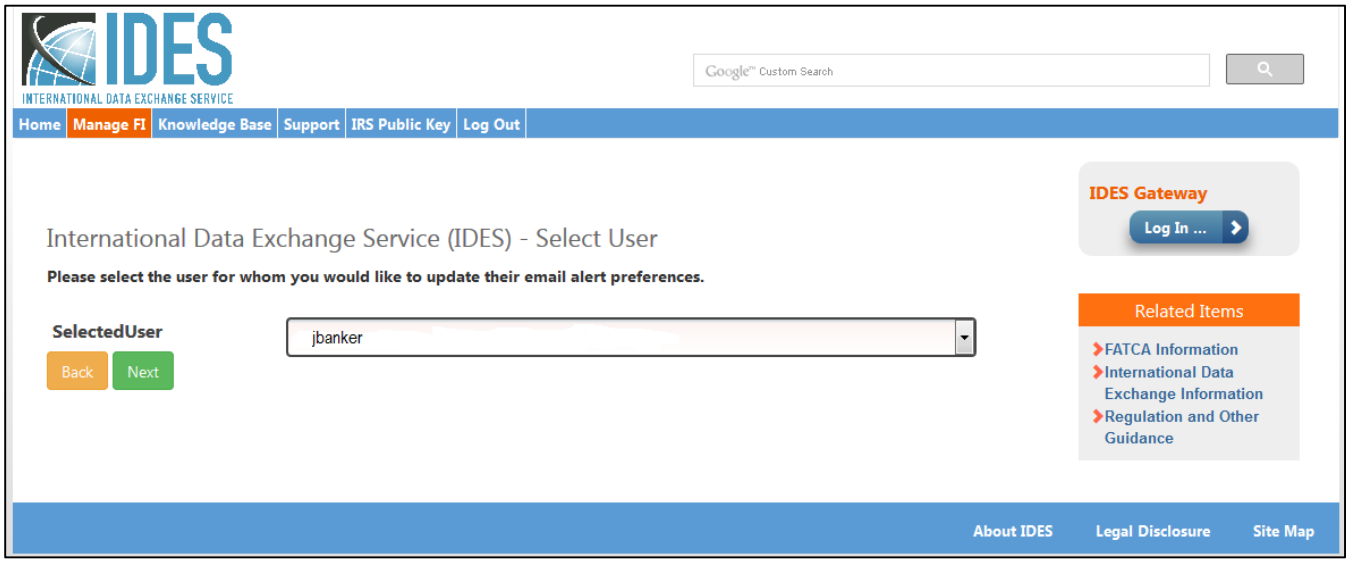


Figure 49

2. **Select User** – Select the User to update their email alert preferences.
3. Click **Next.**

DRAFT

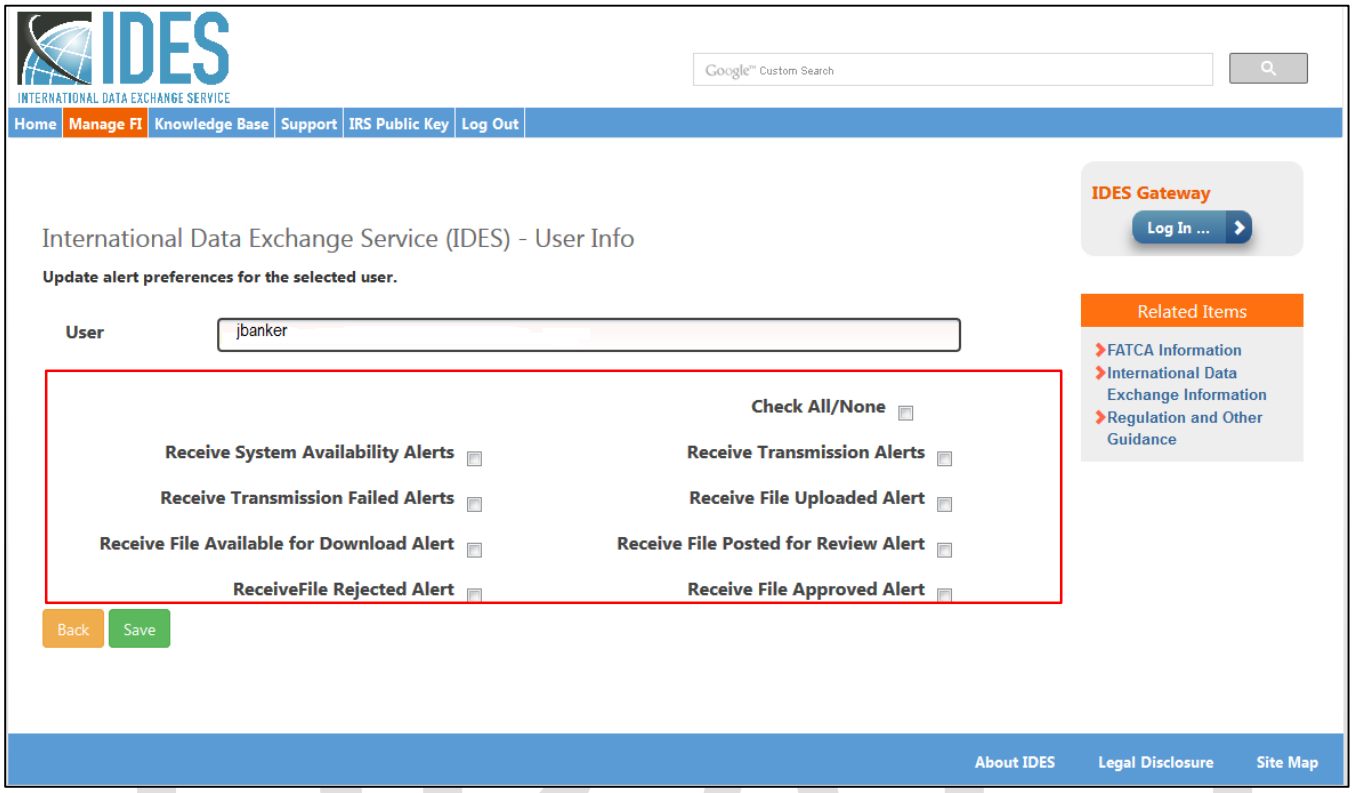


Figure 50

4. **User** – Verify the username that their alert preferences are being updated.
5. Click on the checkbox next to the Alert(s) to receive via email. You can click the **Check All/None** box to choose all alerts or to remove all alerts. There are eight Alert Preferences, refer to Select Alert Preferences for full instructions.
6. Click **Save**.

Create a Metadata File

Metadata is a collection of data about the content and characteristics of the FATCA reporting files. It is used to ensure the transmission archives are correctly processed. The metadata file will be included in the transmission archive and may also be created during the data preparation phase. HCTAs and FIs should create and validate metadata files using the FATCA IDES Metadata XML Schema v1.0.

DRAFT

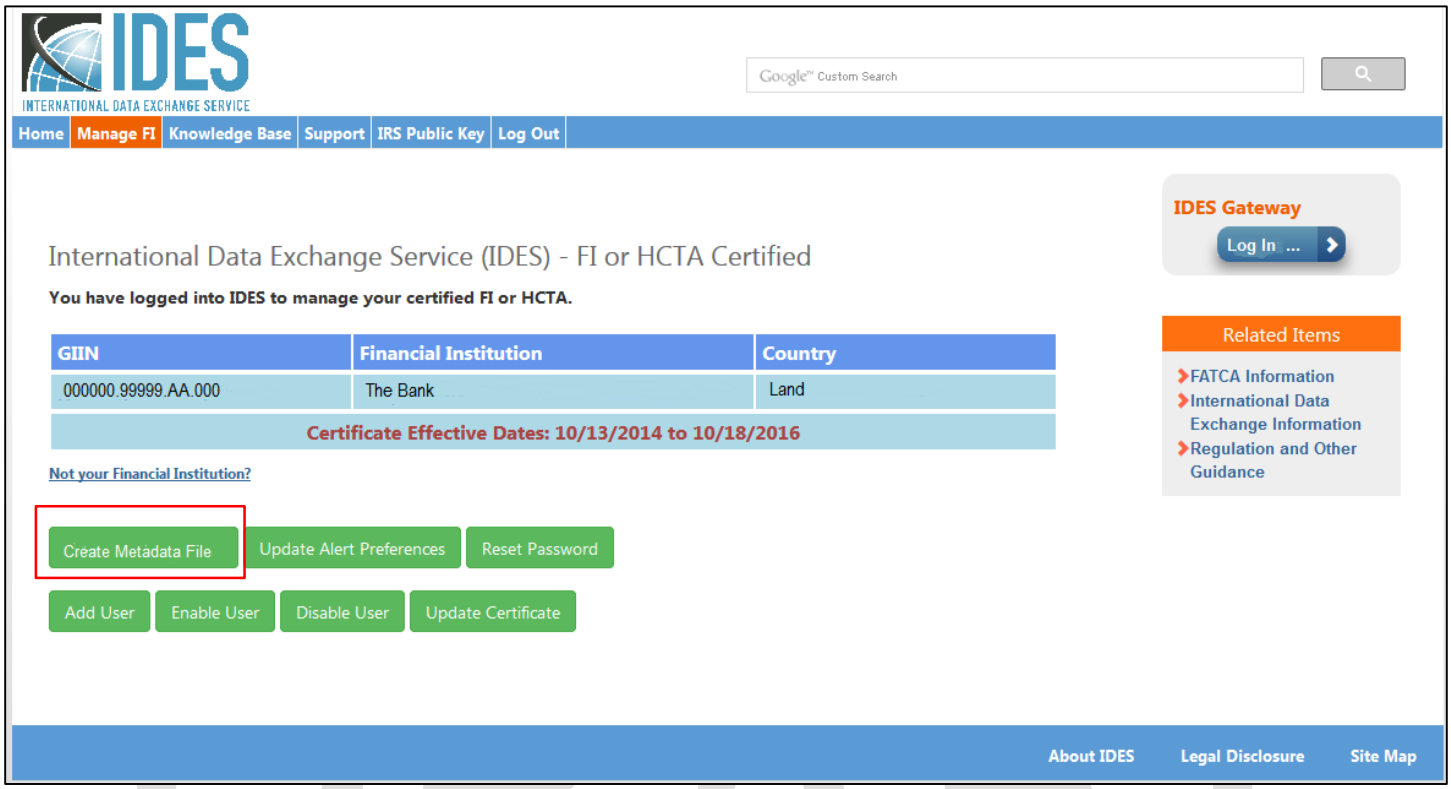


Figure 51

1. Click **Create Metadata File.**

DRAFT

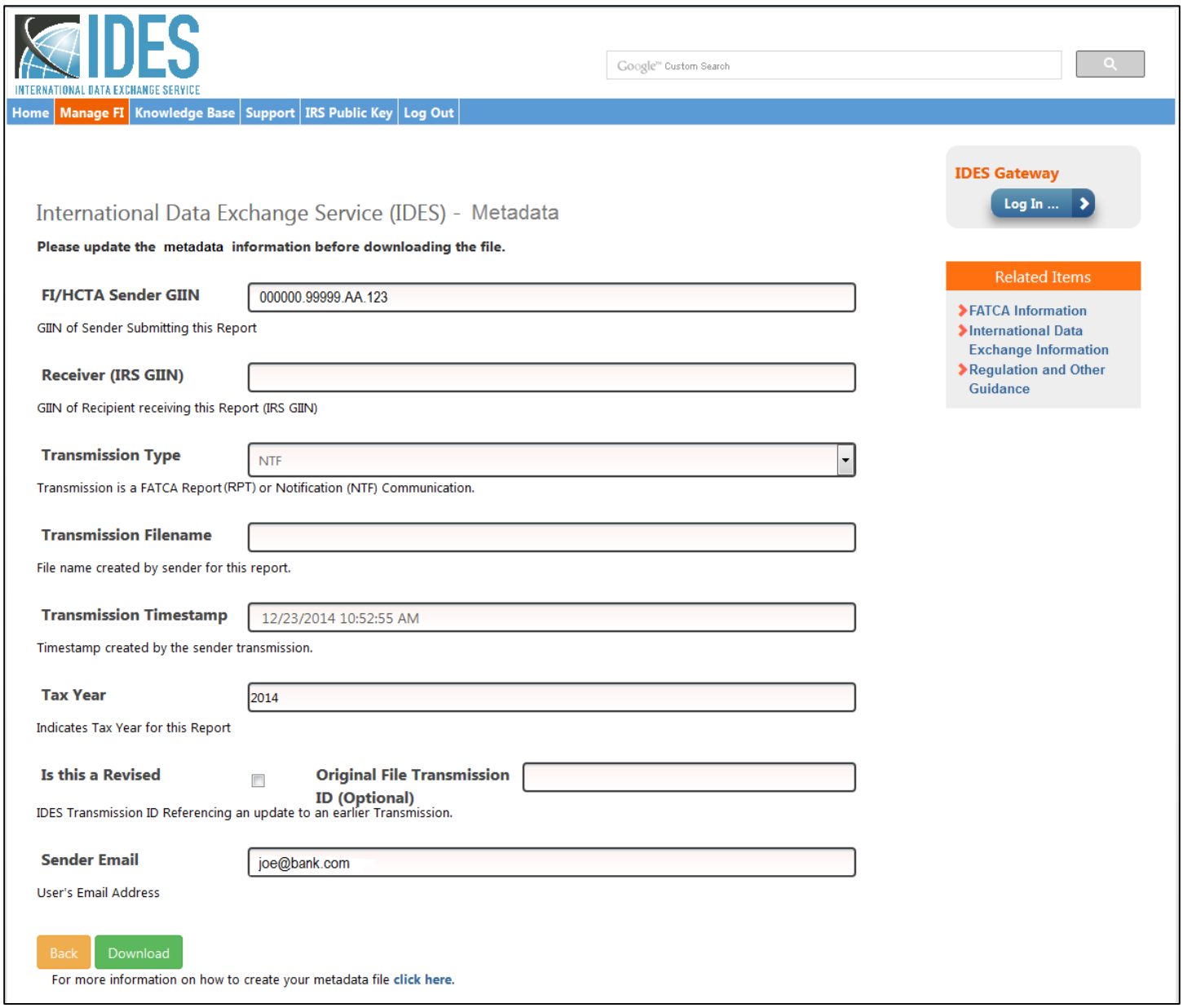


Figure 52

2. **FI/HCTA Sender GIIN** – Enter the Sender GIIN.
3. **Receiver (IRS) GIIN** – Enter the U.S. GIIN.
4. **Transmission Type** – Select the transmission type:
   a. RPT = FATCA Report Communication.
   b. NTF = FATCA Notification Communication.
5. **Transmission Filename** – Enter the SenderFileId or file name of the file being uploaded.
6. **Transmission Timestamp** – Reference the timestamp created by the sender transmission.
7. **Tax Year** – Enter the FATCA reporting data tax year.
8. **Is This a Revised** – Select checkbox if the report is a revision to a file previously uploaded file.
   a. **Original File Transmission ID (Optional)** – Enter the file name of the original file.
9. **Senders Email** – Enter your email address.
10. Click **Download** and review the metadata file.
11. **Save** the file on your computer. The metadata file must be included in the transmission archive. See Preparing the FATCA XML Report for more detail.

.

Reset Password

FI and HCTA Administrators can reset the passwords of all end users under the Administrator account.

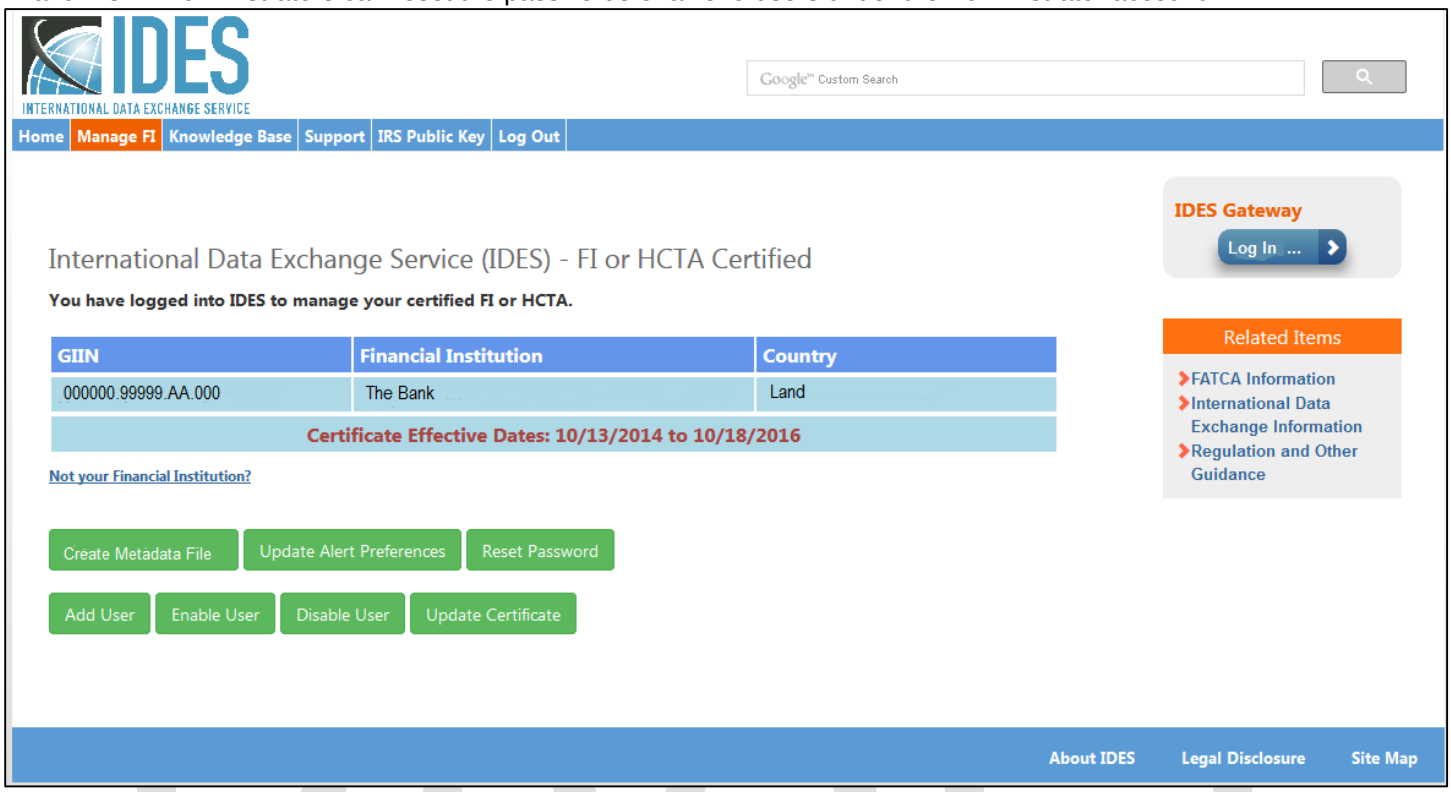


Figure 53

DRAFT

.

1. Click **Reset Password.**

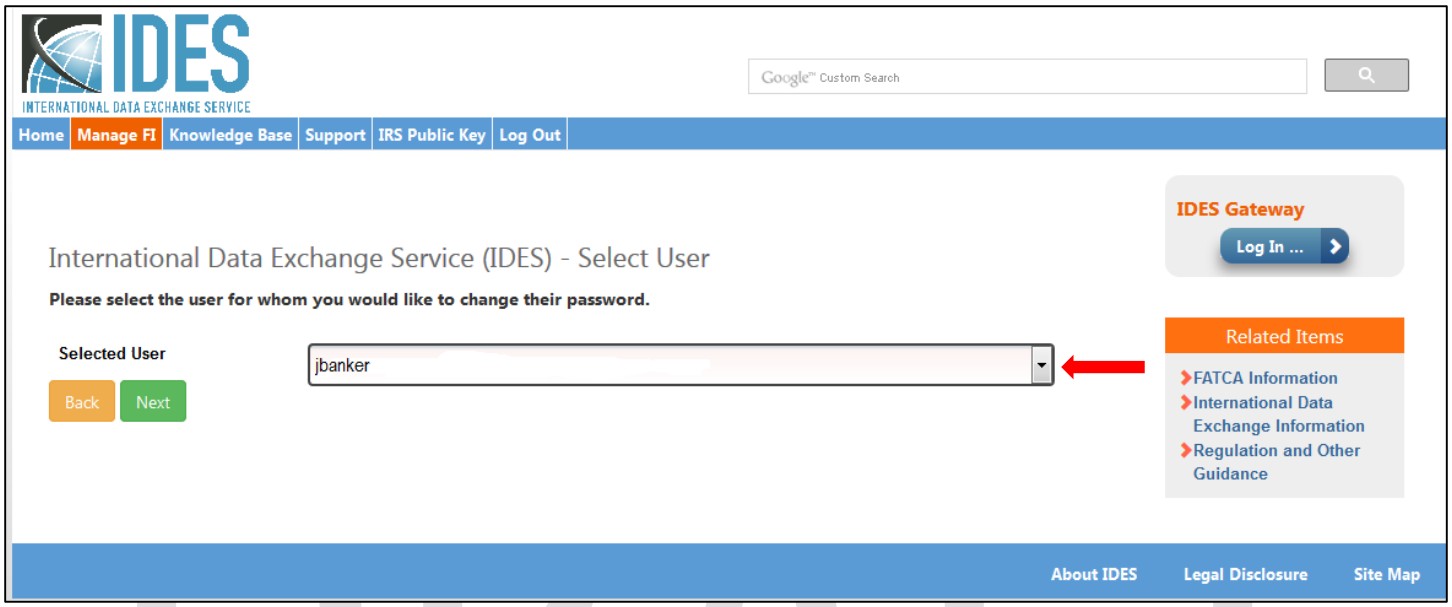


Figure 54

2. **Select User** – Click on the drop down box to select the End user.
3. Click **Next**.

DRAFT

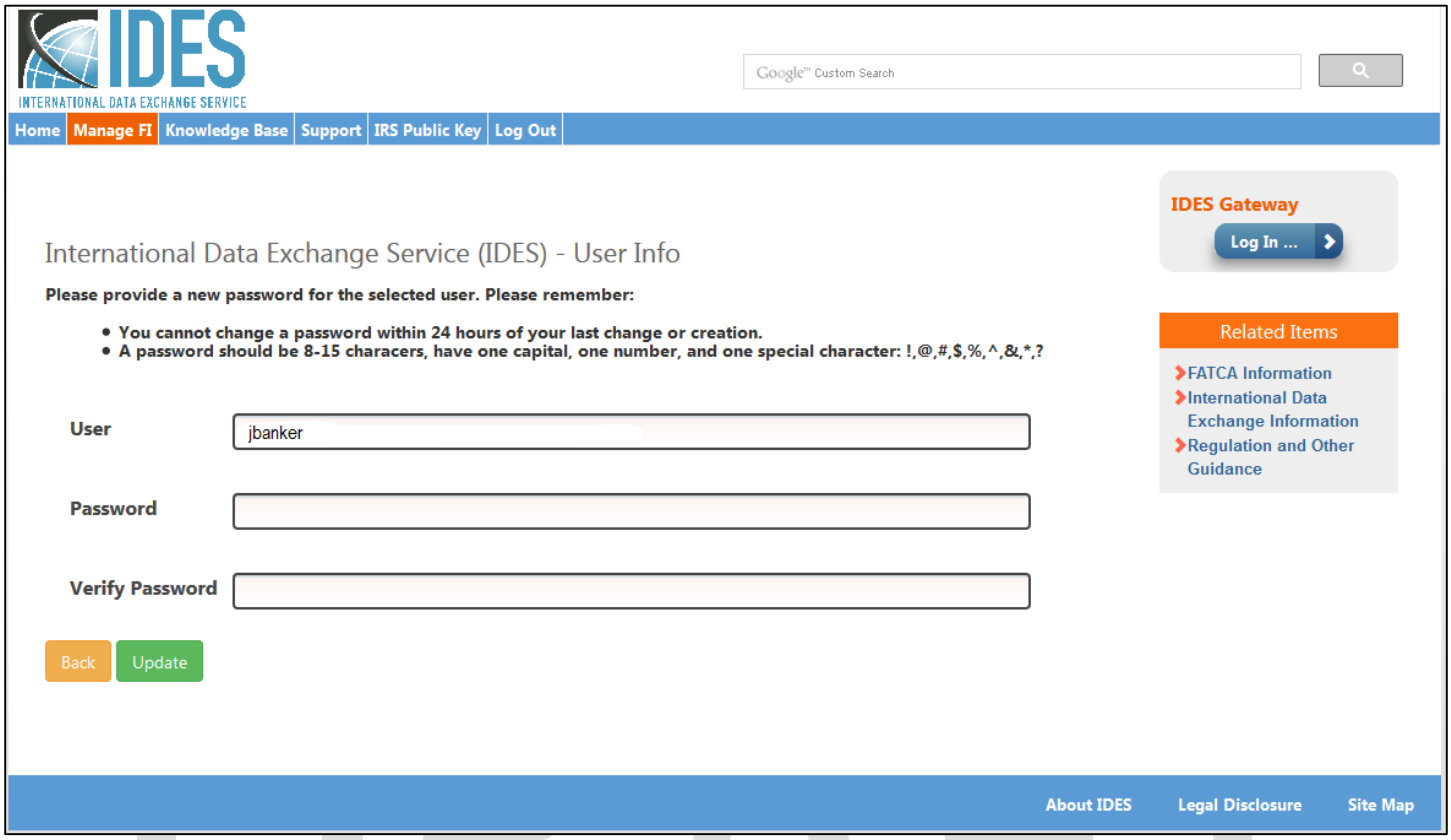


Figure 55

4. **User** – Verify the correct user.
5. **Password** – Enter the new password.
    a. Password Guidelines: The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .). If you enter a password that does not meet the guidelines, you will receive an error message.
6. **Verify Password** – Re-type your password (must match previous entry). If it does not match, you will receive an error message.
7. Click **Update** to complete password update.

DRAFT

Download the IRS Public Key

The IRS Public Key should be included in the transmission archive .zip file that is uploaded through the IDES Gateway.

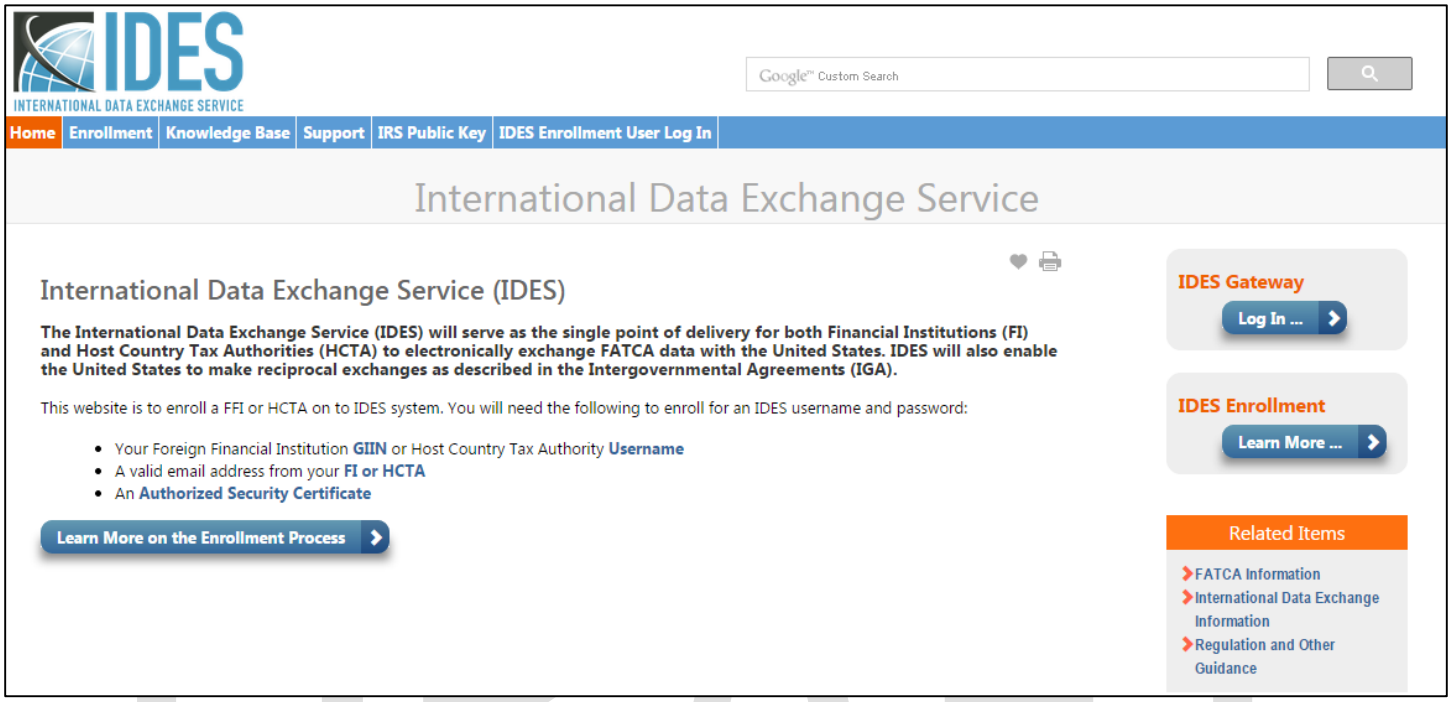


Figure 56

1. From the IDES Enrollment home page, click the **IRS Public Key** tab to begin download of the IRS Public Key Certificate to your computer.

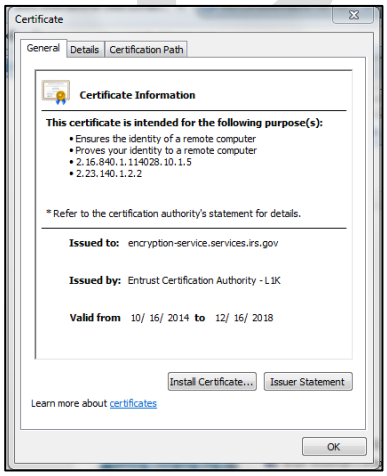


Figure 57

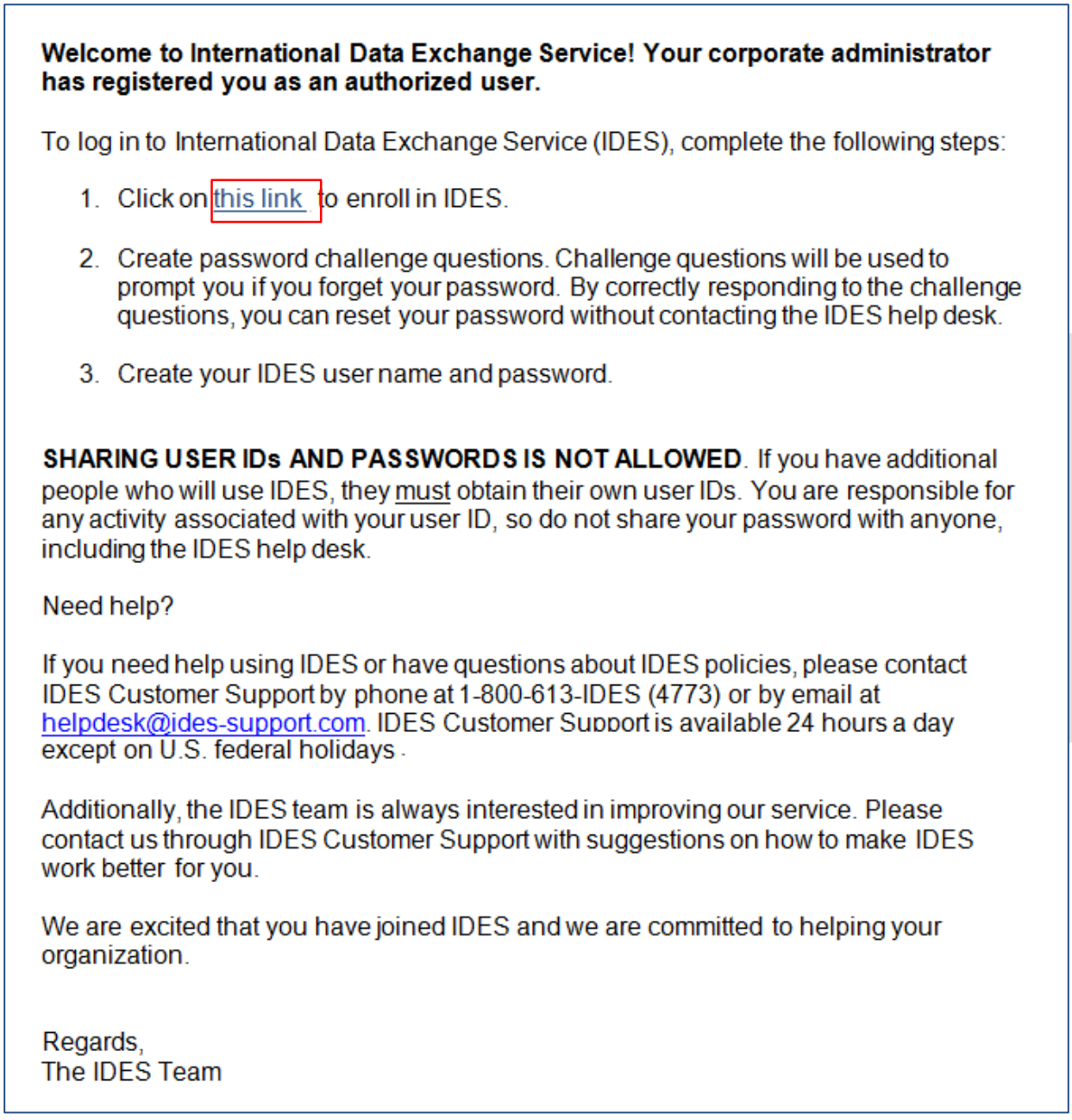
2. This certificate should be included in the FATCA reporting transmission archive you upload and transmit to the IRS via the IDES Gateway.

DRAFT

8. End Users

End users are added by the HCTA or FI Administrator. End users will receive an Email Registration Invitation from the IDES help desk in order to complete the IDES enrollment process. The link within the email is valid for 48 hours.

Create an Account



Welcome to International Data Exchange Service! Your corporate administrator has registered you as an authorized user.

To log in to International Data Exchange Service (IDES), complete the following steps:

1. Click on this link to enroll in IDES.
2. Create password challenge questions. Challenge questions will be used to prompt you if you forget your password. By correctly responding to the challenge questions, you can reset your password without contacting the IDES help desk.
3. Create your IDES user name and password.

SHARING USER IDs AND PASSWORDS IS NOT ALLOWED. If you have additional people who will use IDES, they must obtain their own user IDs. You are responsible for any activity associated with your user ID, so do not share your password with anyone, including the IDES help desk.

Need help?

If you need help using IDES or have questions about IDES policies, please contact IDES Customer Support by phone at 1-800-613-IDES (4773) or by email at helpdesk@ides-support.com. IDES Customer Support is available 24 hours a day except on U.S. federal holidays .

Additionally, the IDES team is always interested in improving our service. Please contact us through IDES Customer Support with suggestions on how to make IDES work better for you.

We are excited that you have joined IDES and we are committed to helping your organization.

Regards,
The IDES Team

Figure 58

1. The new end user will receive a copy of the above email.
2. User will click on **this link** within in the email to complete the IDES enrollment process.

Create Challenge Questions

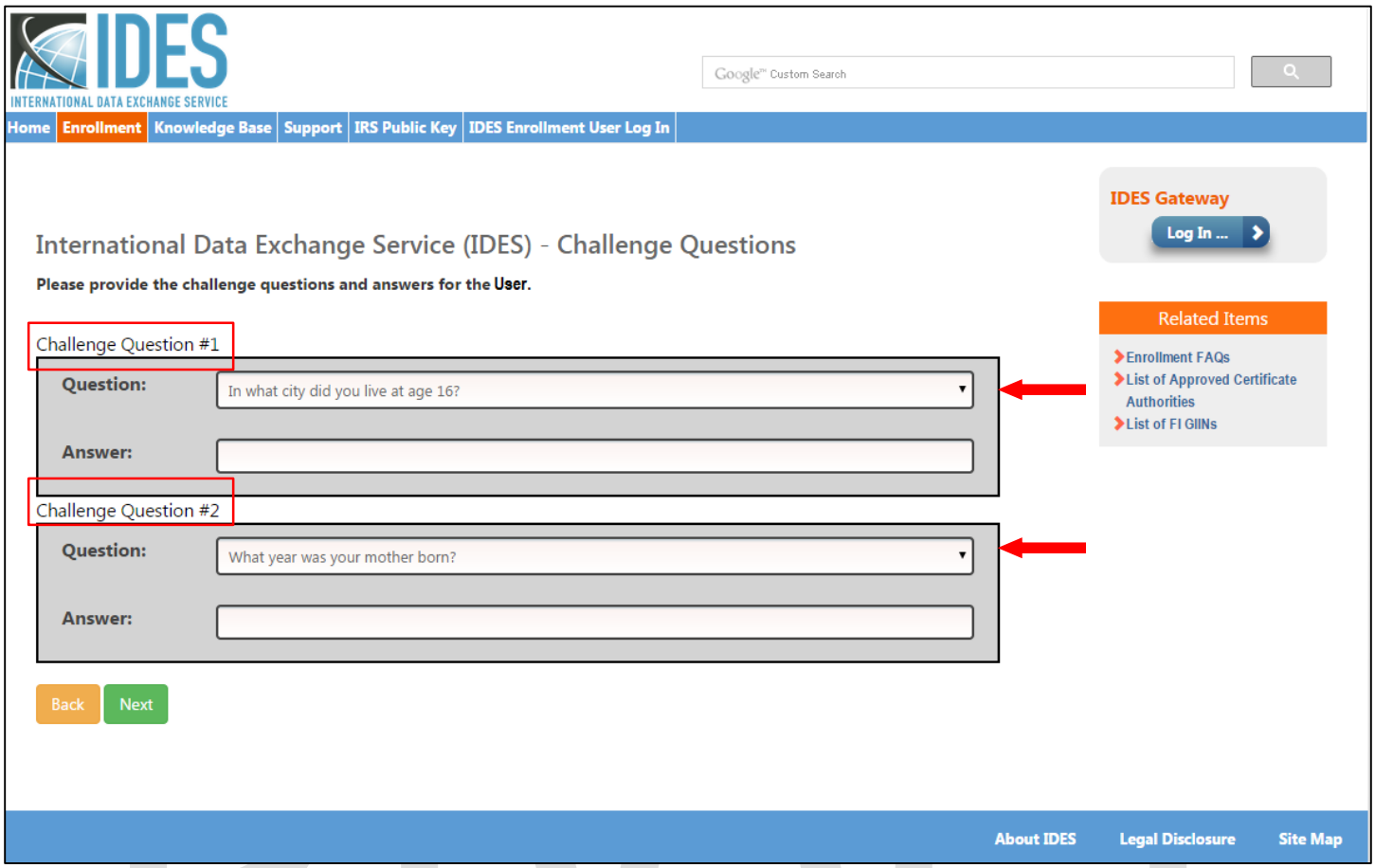


Figure 59

1. **Challenge Question #1**
   c. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   d. Answer: Type a response to the challenge question.
2. **Challenge Question #2**
   c. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   d. Answer: Type a response to the challenge question.
3. Click **Next** to continue and set up a **Username.**

IMPORTANT: Remember to document your answers to your challenge questions. Users will need these to reset password or to contact the IDES Help Desk.

.

Create User Profile

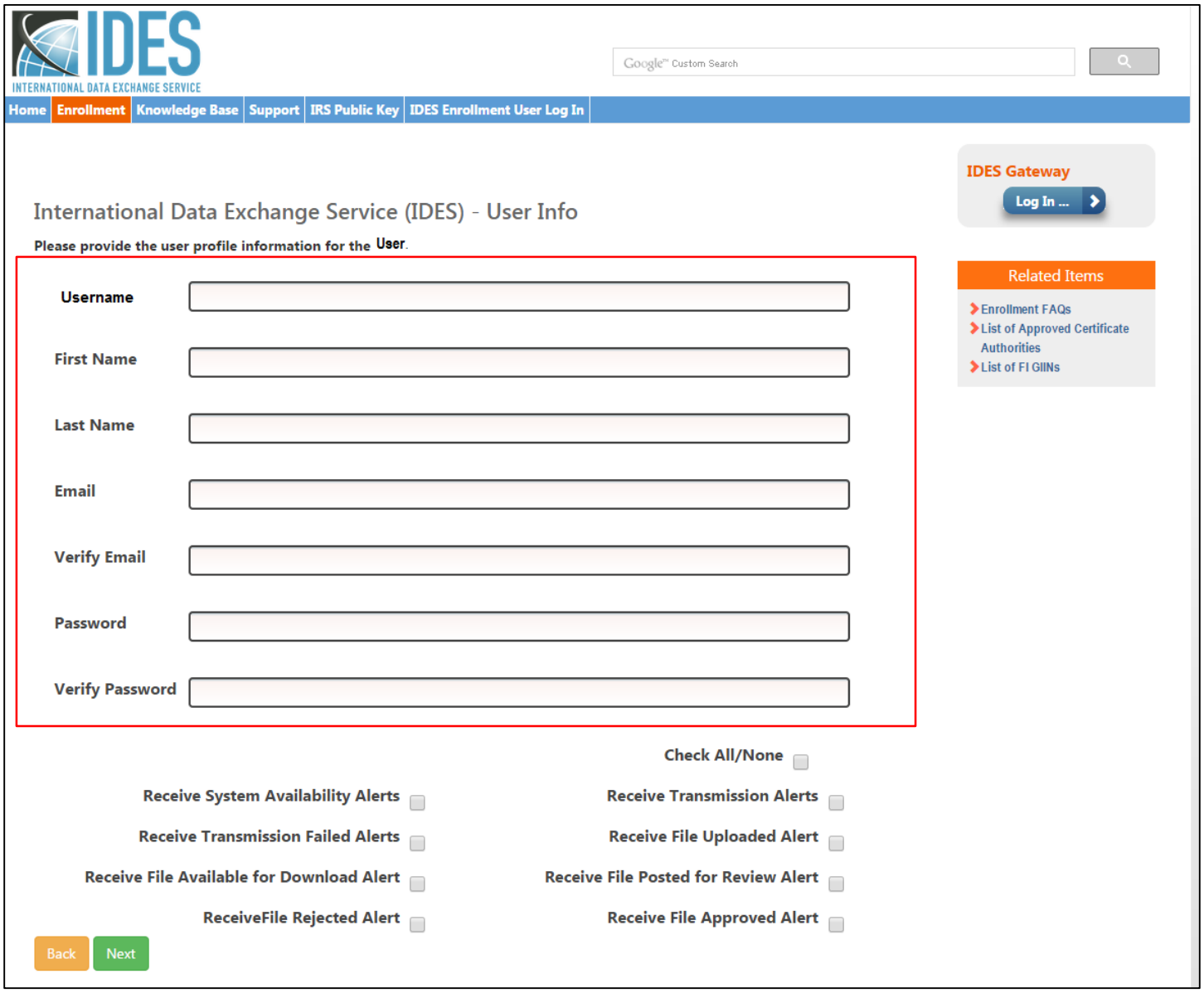


Figure 60

1. **Username** – Enter your new username. We recommend first initial and last name. If the username is already taken you will receive an error message.
2. **First Name** – Enter your first name.
3. **Last Name** – Enter your last name.
4. **Email** – Enter your email address.
5. **Verify Email** – Enter your email address again (must match the previous entry). If it does not match, you will receive an error message.
6. **Password** – Create a valid password.

a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .) .
b. If you enter a password that does not meet the guidelines, you will receive an error message.

7. **Verify Password** – Re-type your password (must match the previous entry). If it does not match, you will receive an error message

Select Alert Preferences

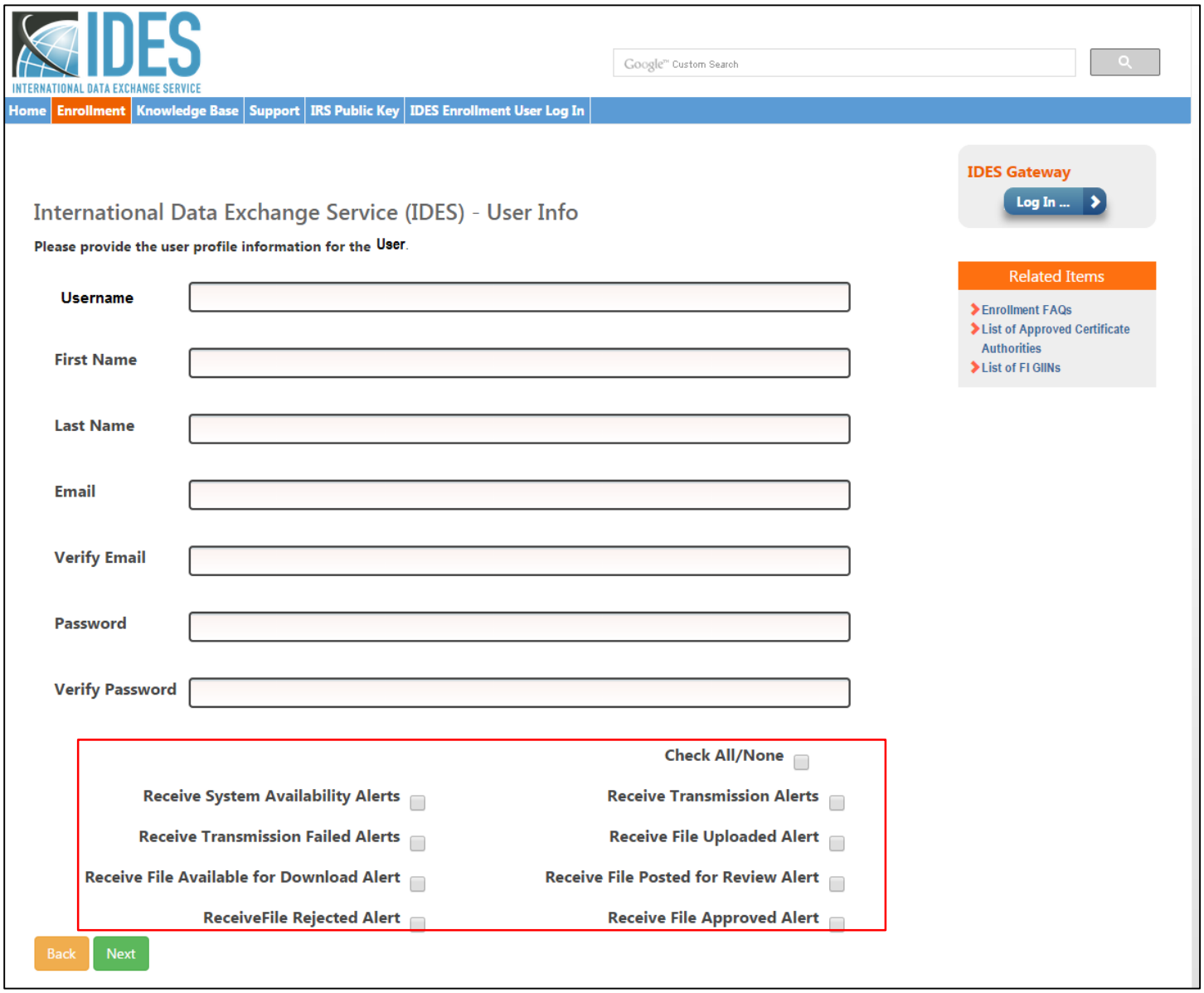


Figure 61

1. Select Alert Preferences – Click on the box next to the alerts you wish to receive by email. You can click the Check All/None box to choose all alerts or to remove all alerts. There are eight Alert Preferences
    a. **Receive System Availability Alerts** – IDES Enrollment and/or IDES Gateway are unavailable.
    b. **Receive Transmission Failed Alert** – transmission uploaded via the IDES Gateway failed for one of several reasons (e.g., virus, encryption validation, naming convention, package content). The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission failed.
    c. **Receive File Available for Download Alert** – the user has a file to download on the IDES Gateway. This is not functional at this time.
    d. **Receive File Rejected Alert** (for Model 1 Option 2 countries) – transmission upload was rejected by the HCTA. The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission was rejected.
    e. **Receive Transmission Alerts** – Receive all IDES Alerts (See Alerts **b,c,d,f,g,h**).
    f. **Receive File Uploaded Alert** – received transmission is uploaded to the IRS for review.
    g. **Receive File Posted for Review Alert** (for Model 1 Option 2 countries) – sent to the HCTA when an FFI uploads a report.
    h. **Receive File Approved Alert** (for Model 1 Option 2 countries) – sent after HCTA has approved the FFI file.
2. Click **Next** to continue to complete enrollment process.

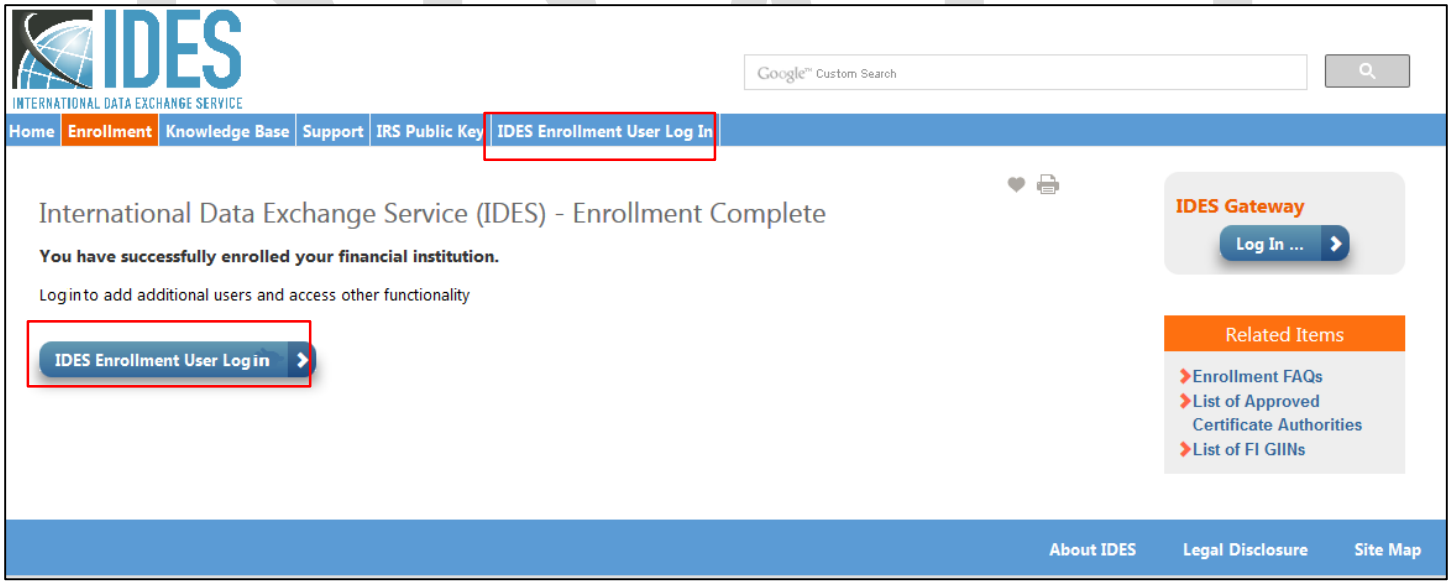


Figure 62

3. You have completed the enrollment process as an end user. You will also receive an email from the IDES help desk that verifies your authorization to access IDES Gateway.
4. Click **IDES Enrollment User Log In** to log in as an end user.

IDES Enrollment User Log In

1. Access the IDES Enrollment site at www.IDES-Support.com.

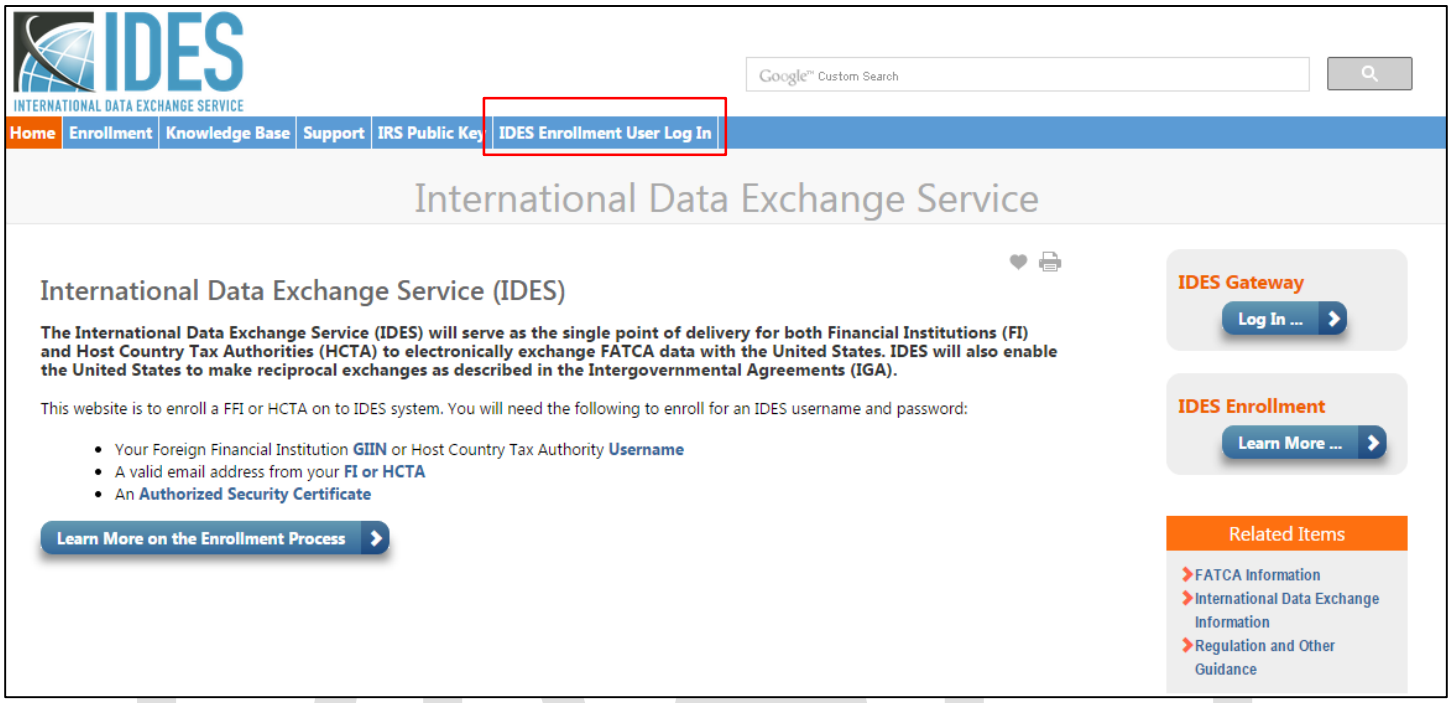


Figure 63

2. Click on the **IDES Enrollment User Log In** tab.

DRAFT

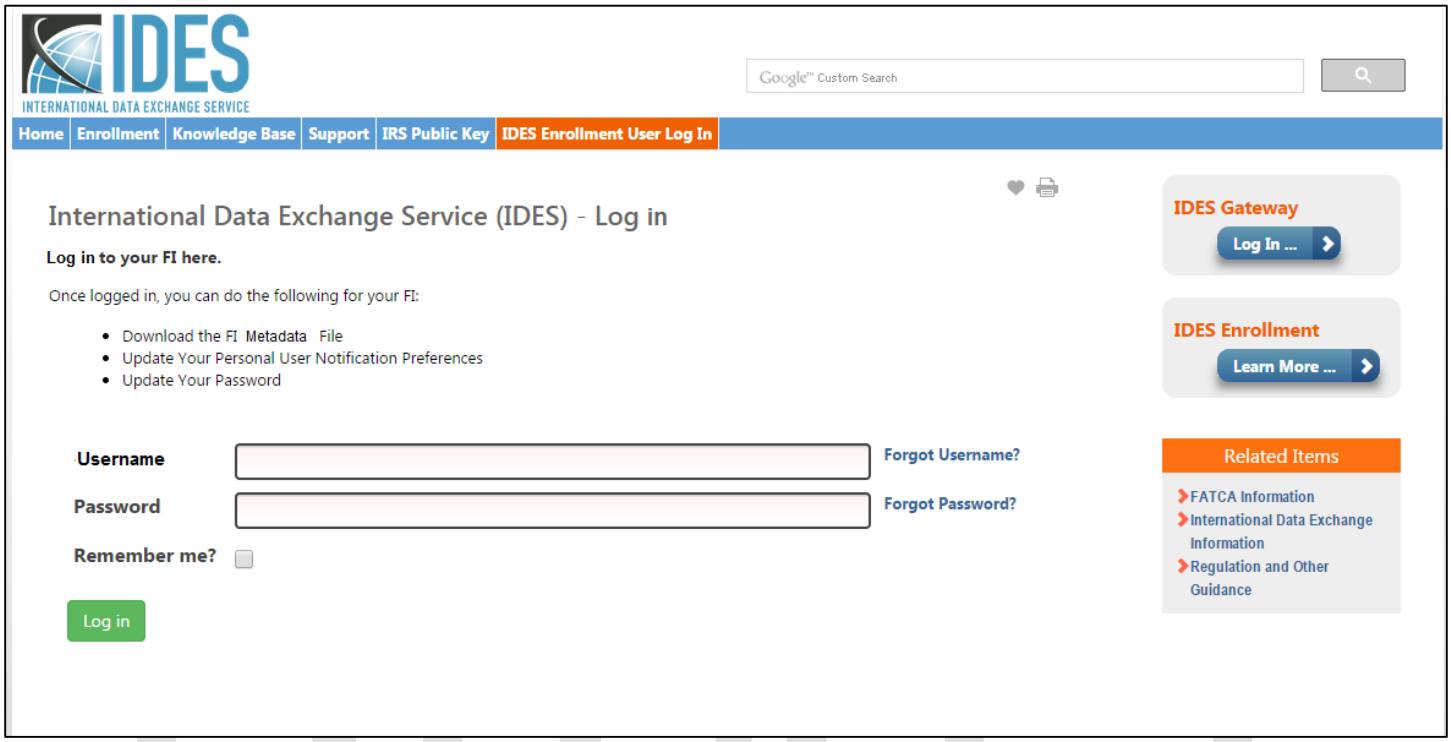


Figure 64

3. **Username** – Enter your Username
4. **Password** – Enter Password
5. Click **Log in**.

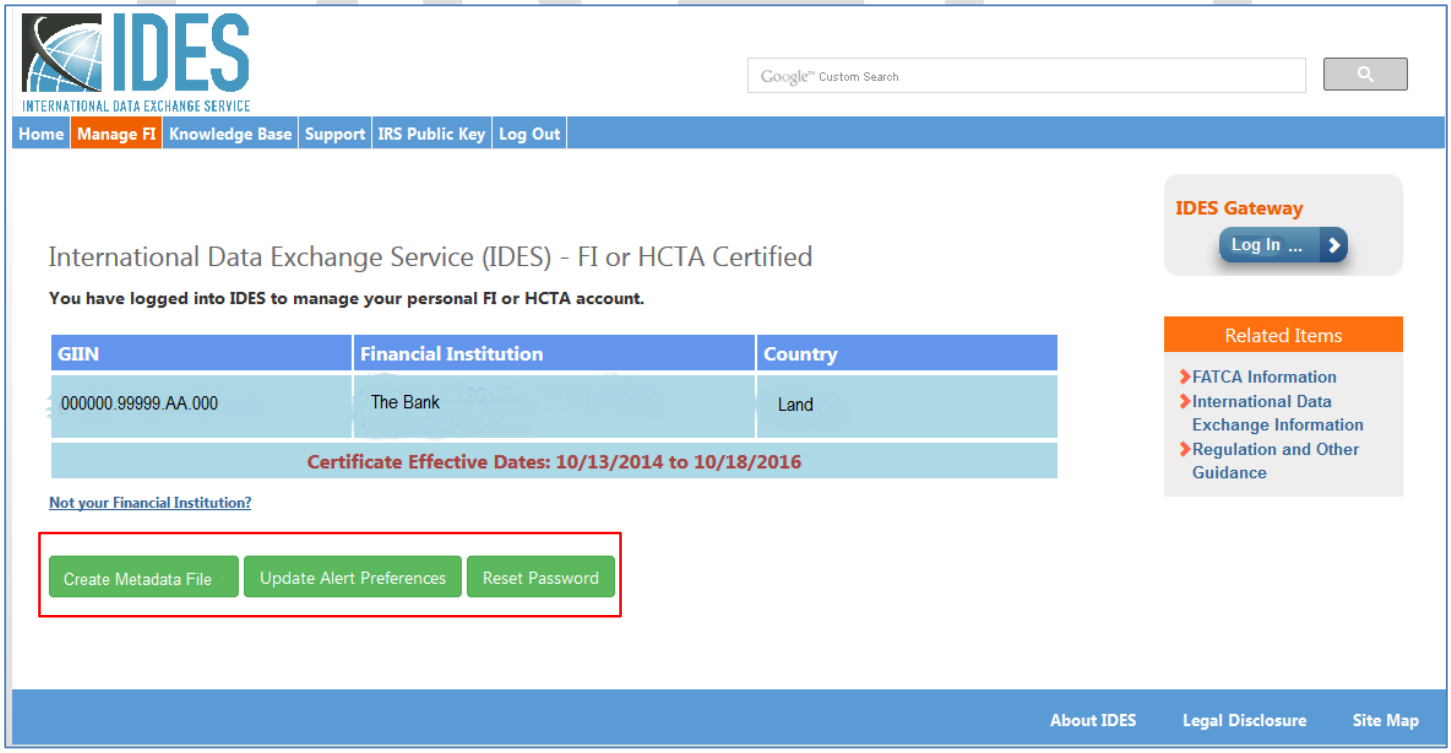


Figure 65

6. You are now signed in. You can perform three functions from this screen:
   a. **Create a Metadata File**.

DRAFT

b. **Update Alert Preferences**.
c. **Reset Password**.

Create a Metadata File

Metadata is a collection of data about the content and characteristics of the FATCA reporting files. It is used to ensure the transmission archives are correctly processed. The metadata file will be included in the transmission archive and may also be created during the data preparation phase. HCTAs and FIs should create and validate metadata files using the FATCA IDES Metadata XML Schema v1.0.

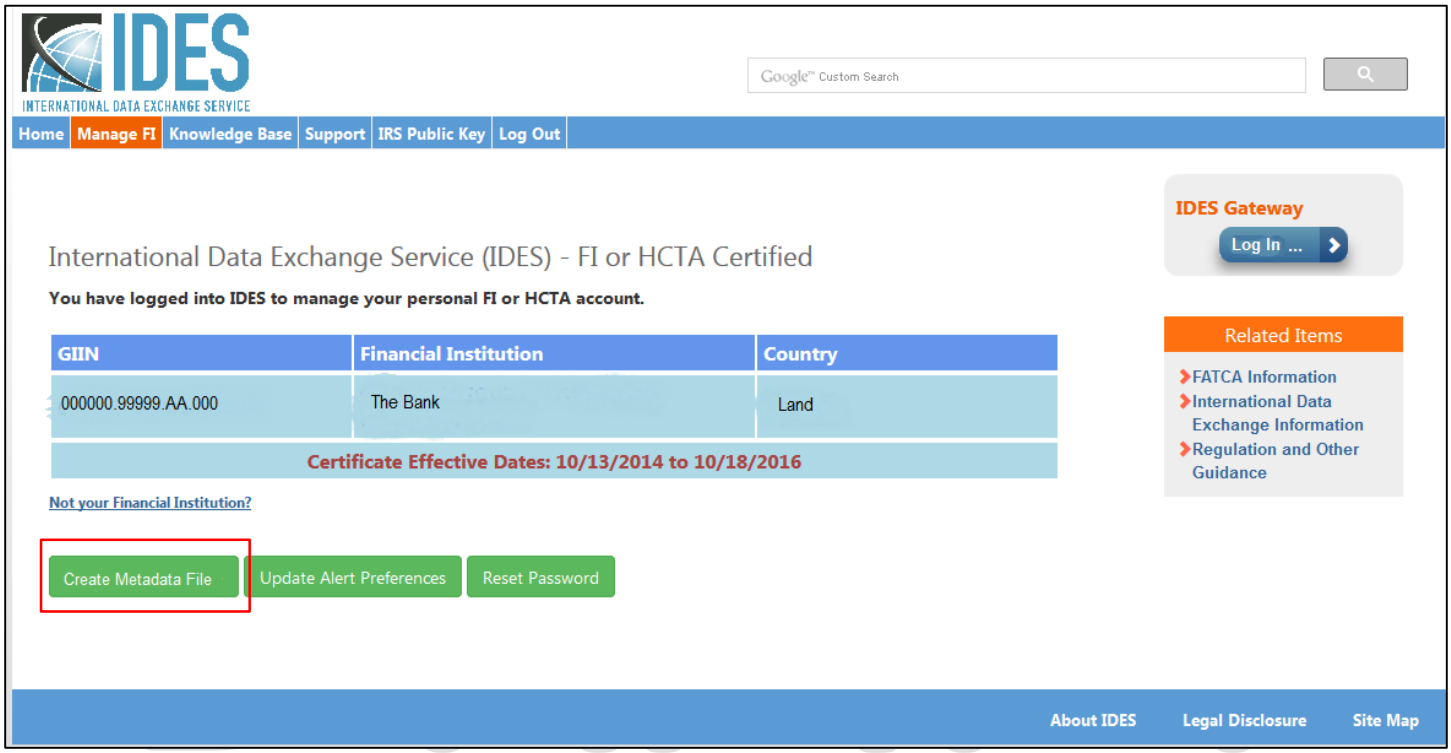


Figure 66

1. From the **Manage FI** tab, click **Create Metadata File.**
2. Refer to Create a Metadata File for full instructions.

Update Alert Preferences

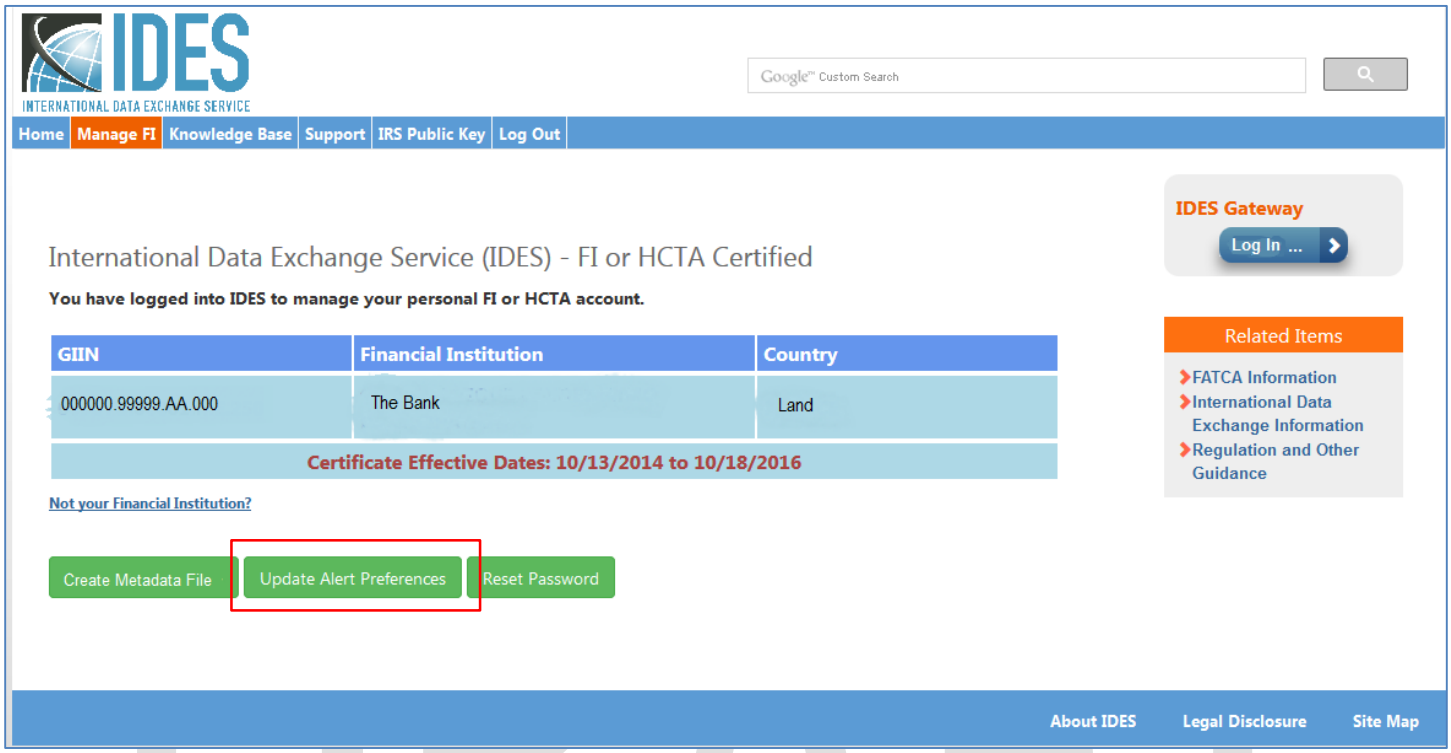


Figure 67

1. From the **Manage FI** tab, click **Update Alert Preferences.**

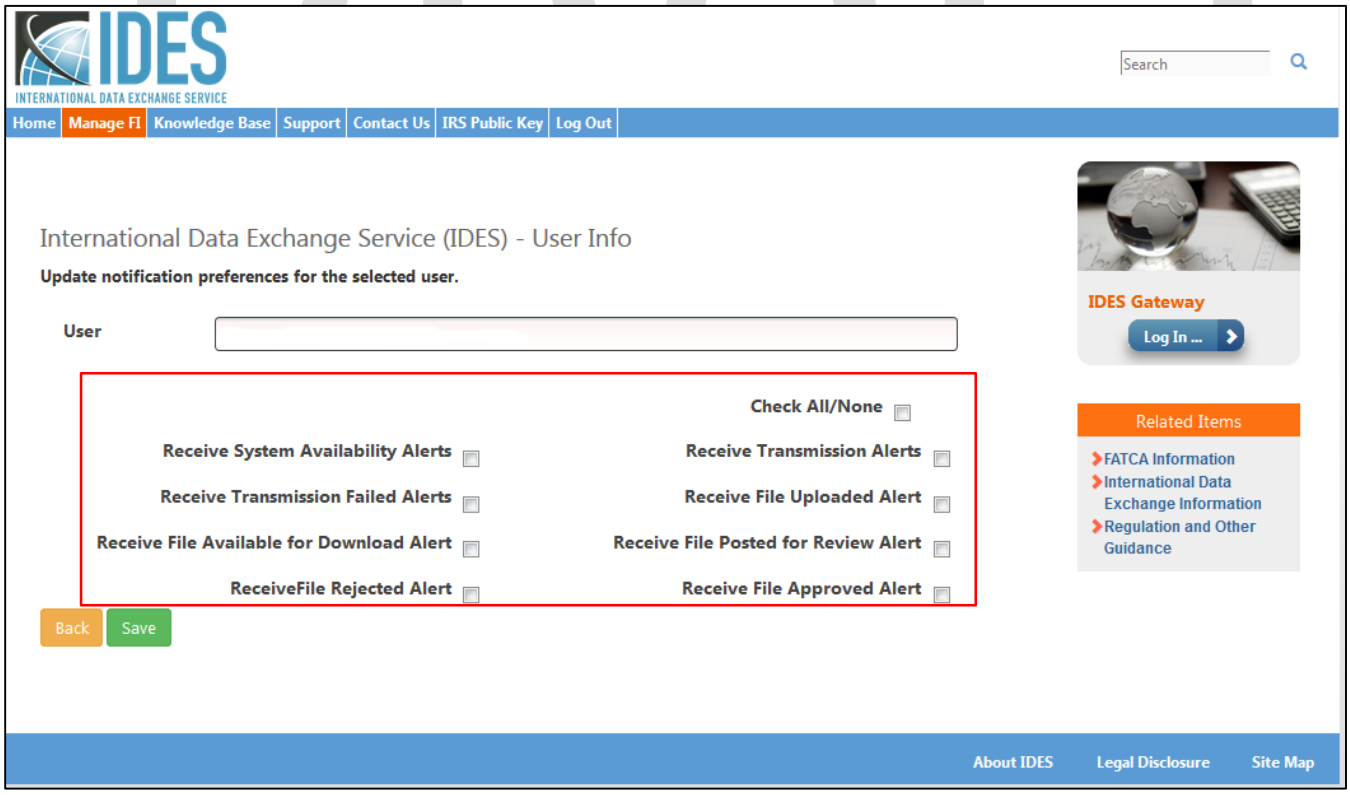


Figure 68

DRAFT

2. Your Username will appear in the User field
3. Select the Alert(s) that you want to receive by email. If you want to receive all alerts click the **Check All/None** box. Clicking it again will remove all alerts. See Select Alert Preferences for full instructions.

DRAFT

Reset Password

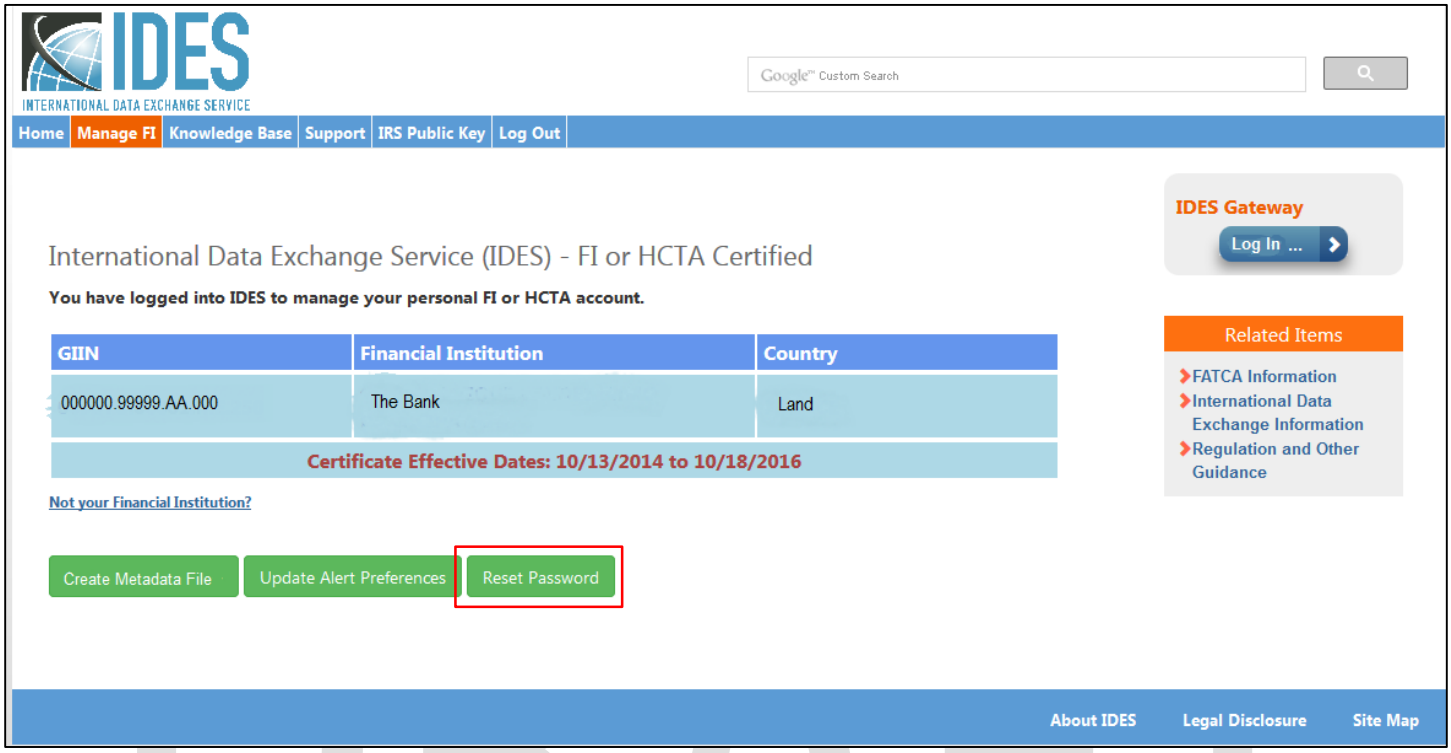


Figure 69

1. From the **Manage FI** tab, click **Reset Password**

DRAFT

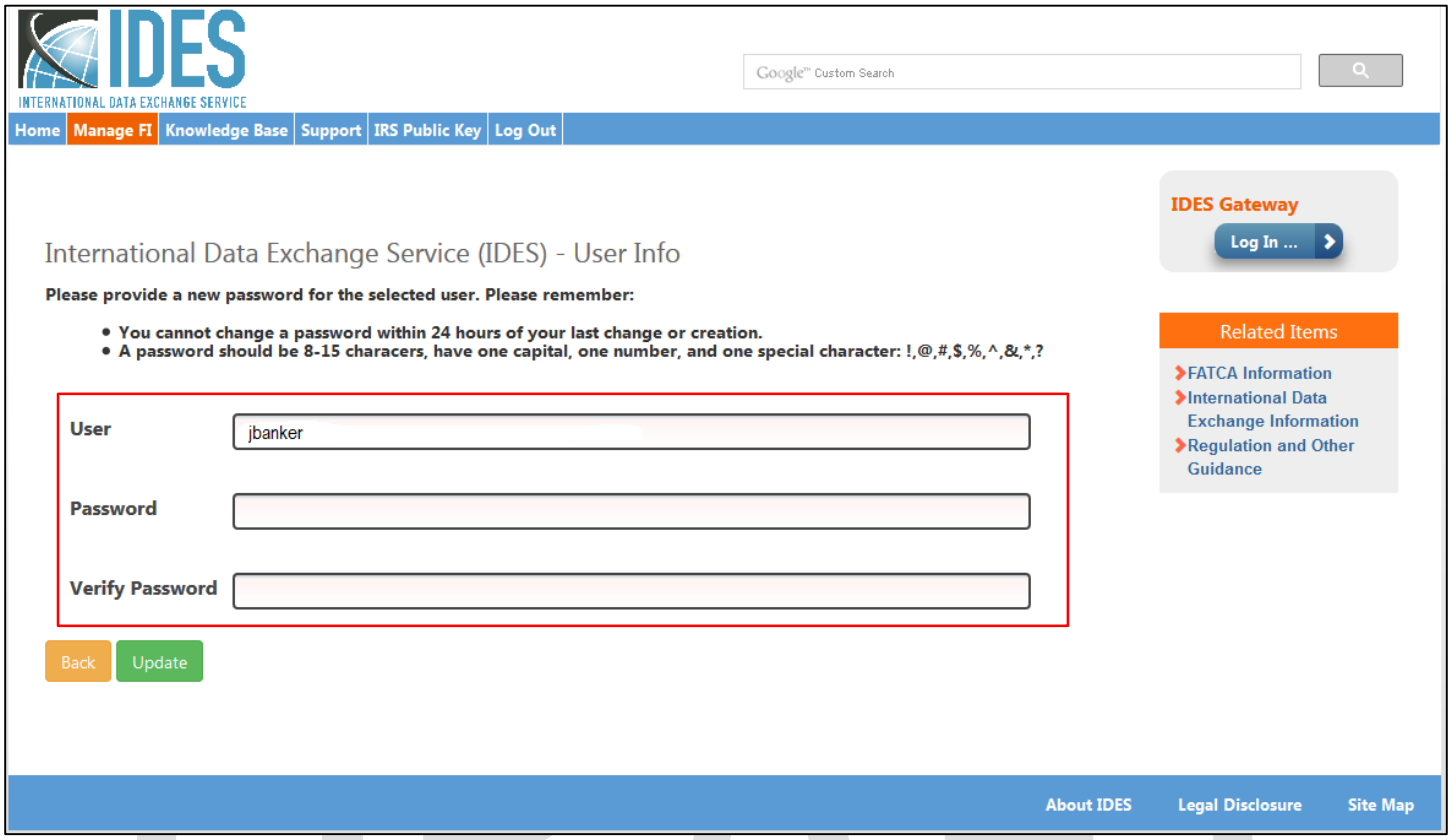


Figure 70

2. **User** - Verify your username.
3. **Password** – Enter a new password.
    a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .) . If you enter a password that does not meet the guidelines, you will receive an error message.
4. **Verify Password** - Re-type your password (must match previous entry). If it does not match, you will receive an error message.
5. Click **Update** to complete password update.

Forgot Username

If an end user forgets their username, they can request a Username Reminder email.

DRAFT

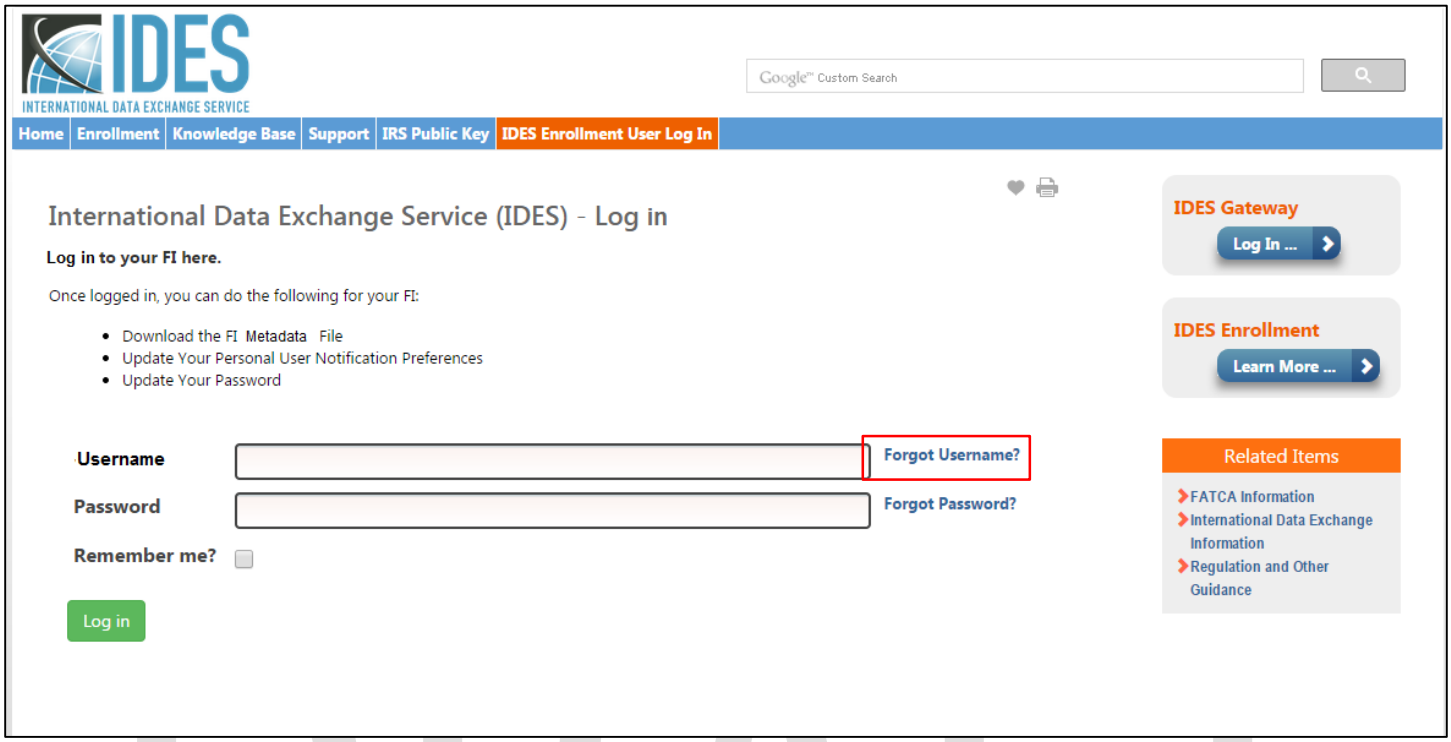


Figure 71

1. Select **IDES Enrollment User Log In** tab, click **Forgot Username?**

DRAFT

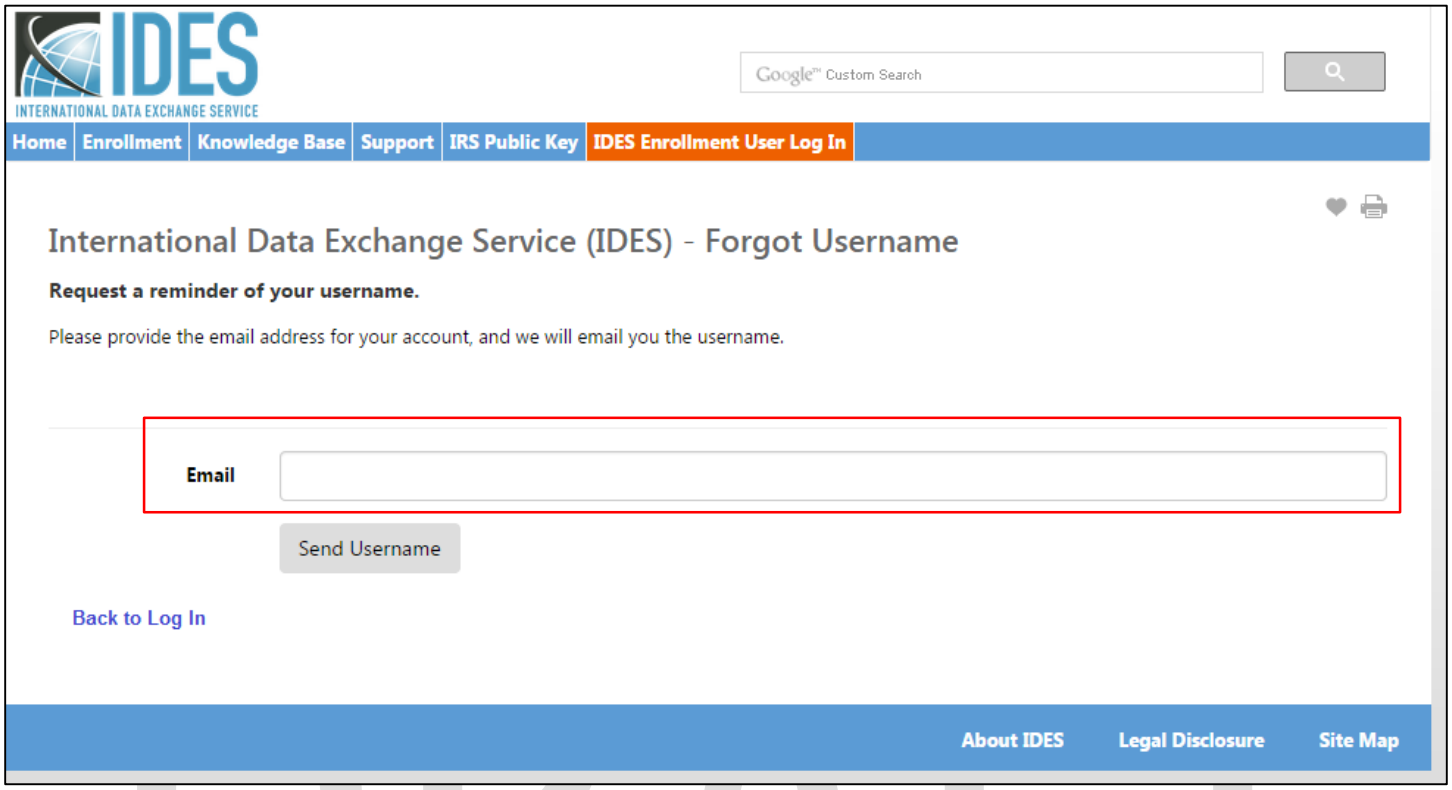


Figure 72

2. **Email** – Enter the email address used to register on the IDES enrollment site.
3. Click **Send Username**.

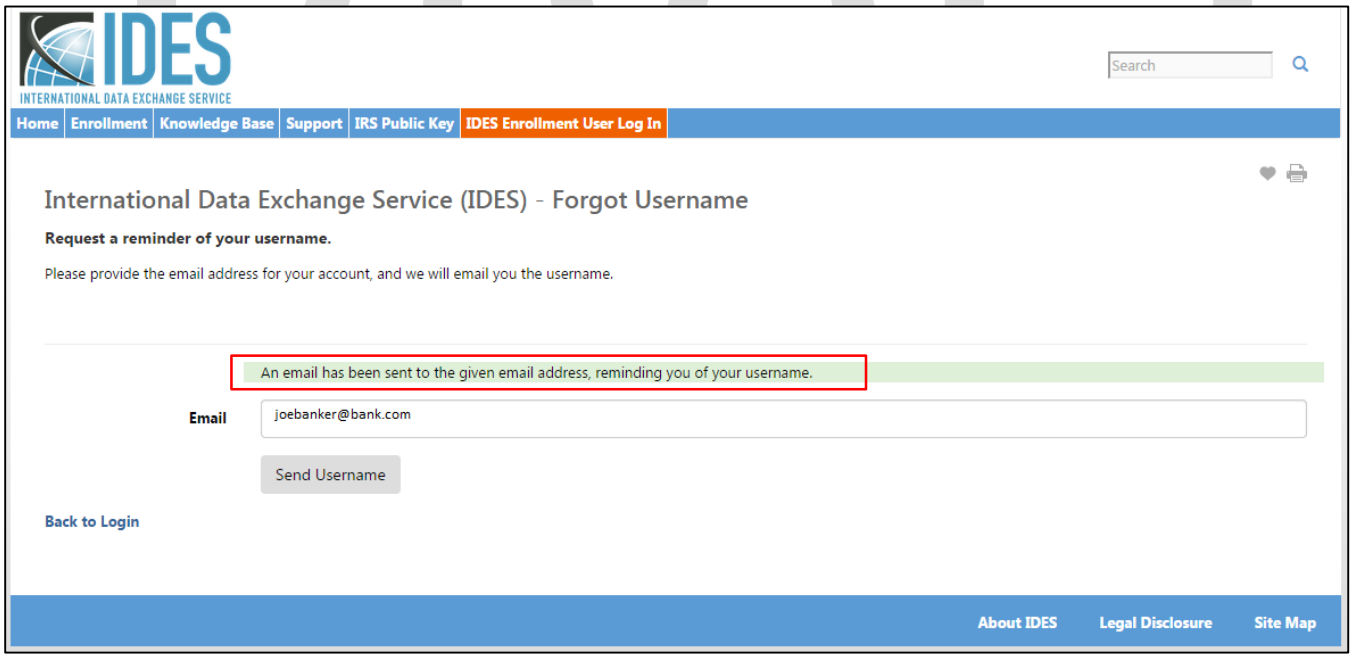


Figure 73

4. Confirmation page showing that username reminder email was sent.

DRAFT

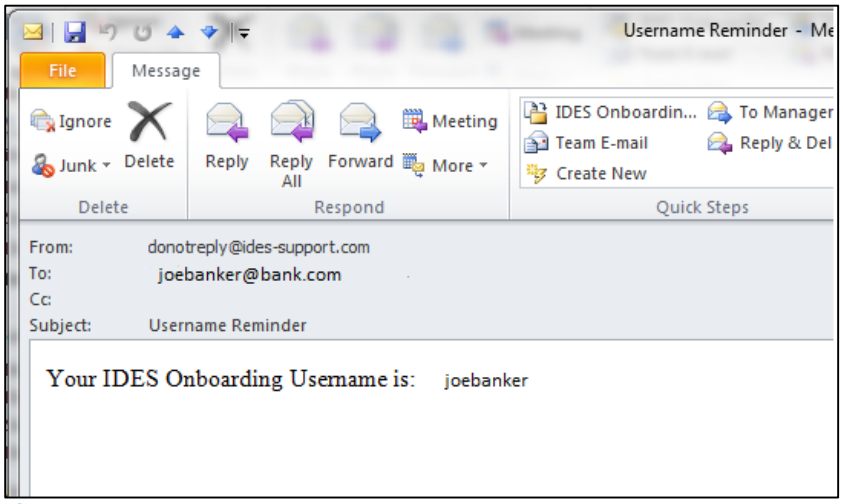


Figure 74

5. Check your email for a copy of Username Reminder email. Return to the IDES enrollment home page and select the **IDES Enrollment User Log In** tab.

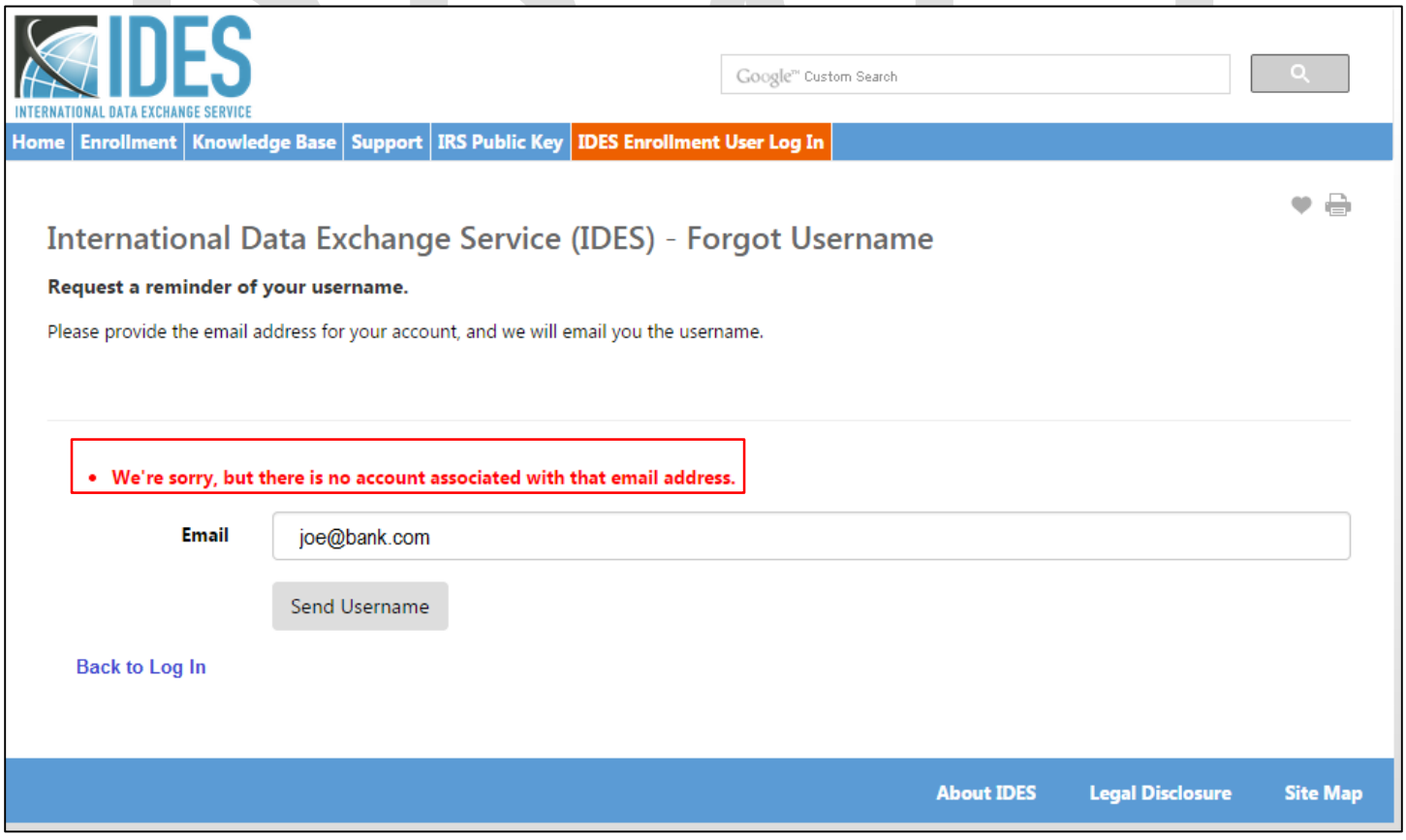


Figure 75

Note: If there is not an IDES account associated with the email address entered, you will receive an error message Enter the same email that was used for enrollment. If you still receive the error, after entering the correct email, contact the Help Desk.

Forgot Password

Passwords can be reset on the **IDES Enrollment User Log In** tab.

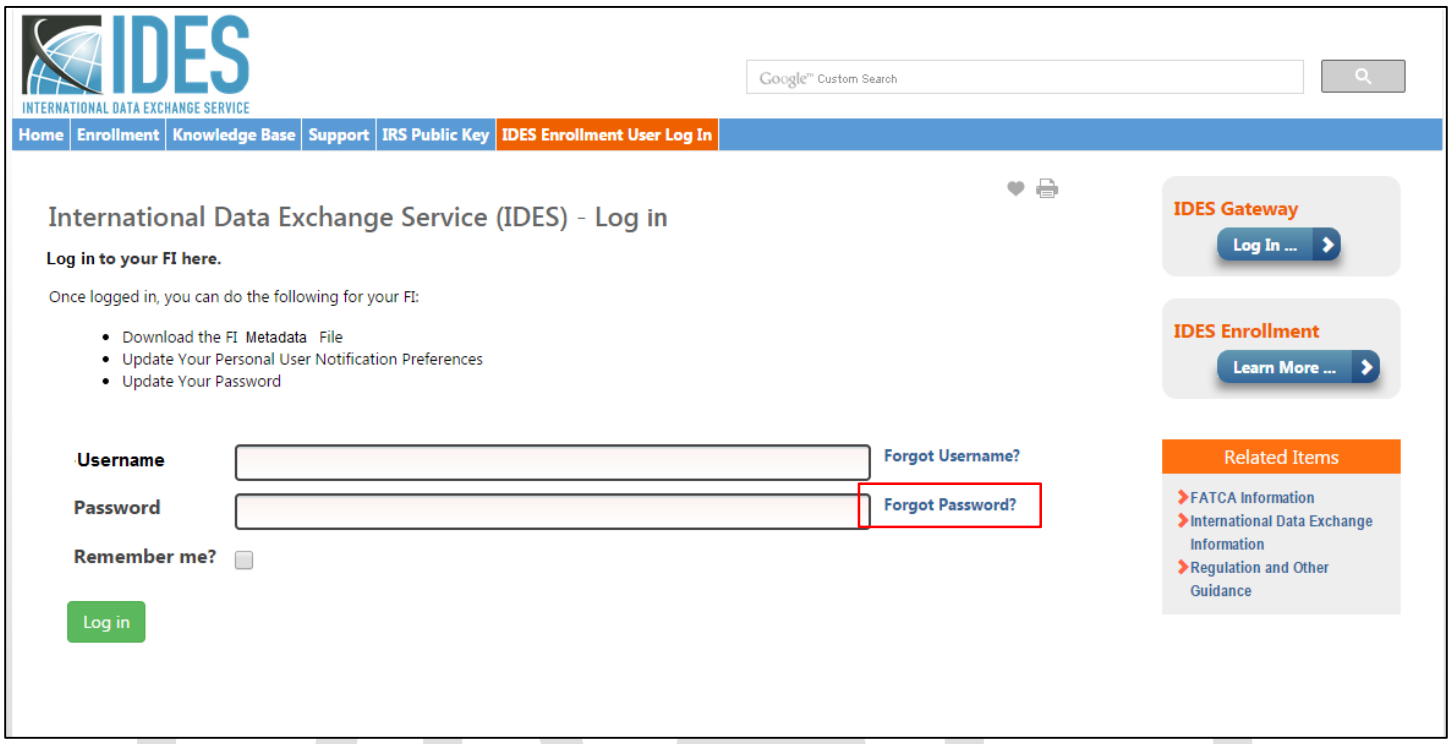


Figure 76

1. Select **IDES Enrollment User Log In** tab, click on **Forgot Password?**

DRAFT

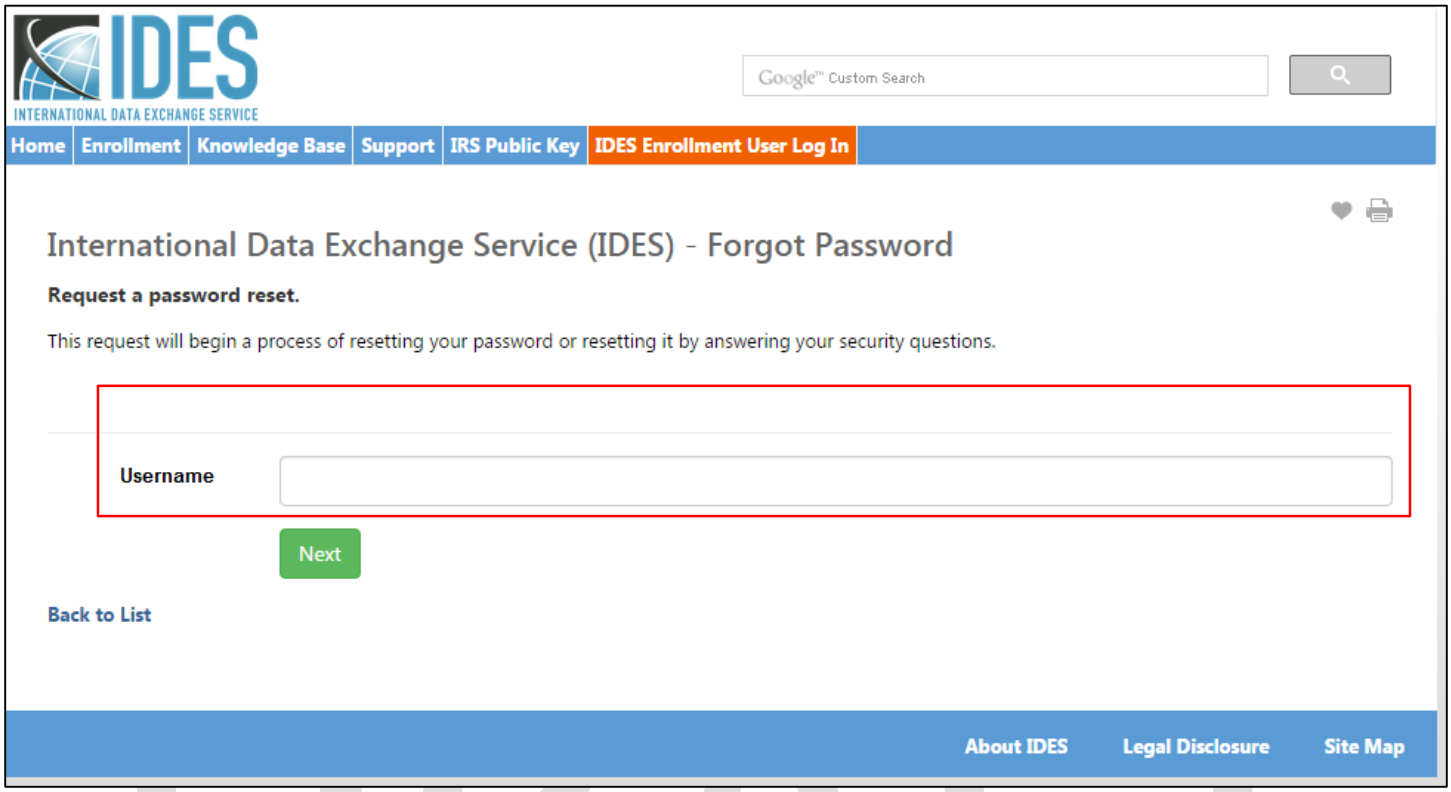


Figure 77

2. **Username** – Enter your username.
3. Click **Next** to continue.

DRAFT

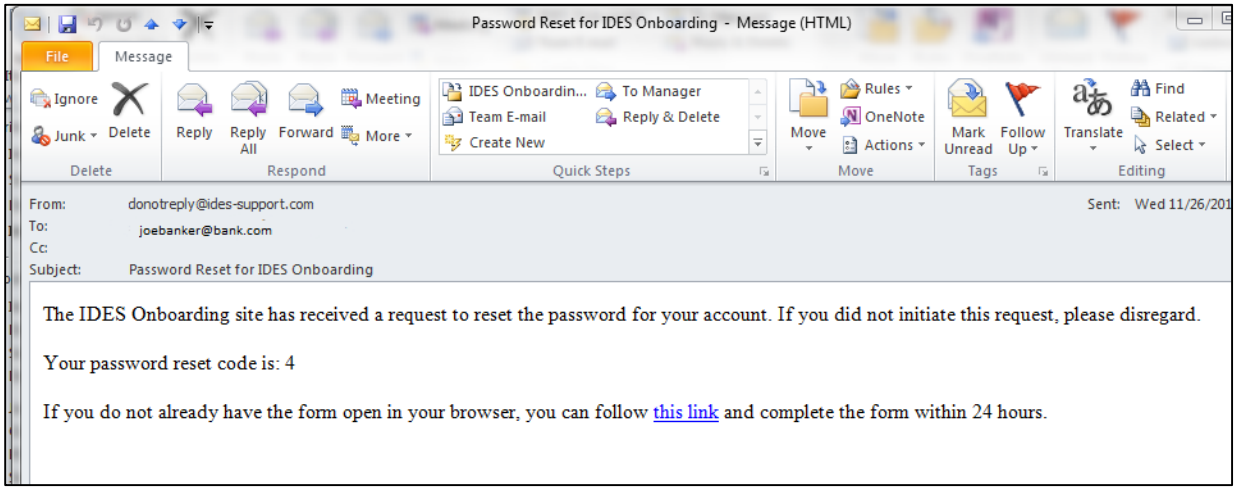


Figure 78

4. An email will be sent to the email address provided during enrollment. The email will contain a reset code needed to reset the user's password.

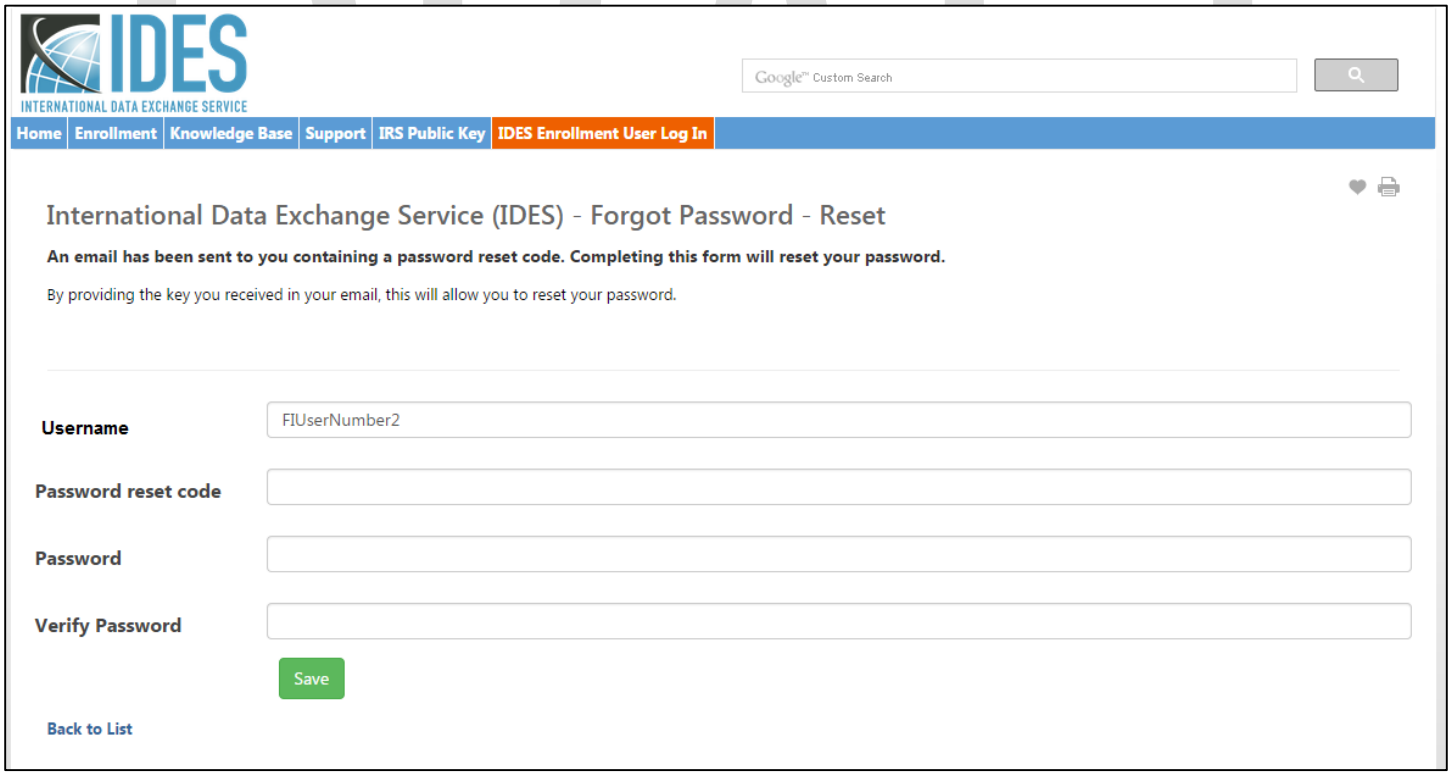


Figure 79

5. **Password Reset Code** – Enter the reset code you received in your email.
6. **Password** – Enter your new password.
   a. The Password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .). If you enter a password that does not meet the guidelines, you will receive an error message.

7. **Verify Password** – Re-type your password (must match previous entry). If it does not match, you will receive an error message.
8. Click **Save** and return to the **IDES Enrollment User Log In** tab to log in with your new password.

9. Preparing the FATCA XML

Overview

This section describes how to prepare and transmit a FATCA data file to IDES. Before you begin, you must have a valid certificate from an IRS approved certificate authority.

Preparing the FATCA XML File

These instructions are preliminary and may change with maintenance updates to the system. IDES will only accept files in .zip format. Each archive will contain either three or four files depending on the IGA Model or type of agreement.

Steps	Process	File Naming Convention
---	Obtain a digital certificate from an approved Certificate Authority (CA). See Section 3, Obtaining a Digital Certificate	Not applicable
1	Prepare and validate the FATCA XML file Digitally sign the file	[SenderGIIN]_Payload.xml
2	Compress the FATCA XML file with compatible zip utility	[SenderGIIN]_Payload.zip
3	Encrypt the FATCA XML file with AES-256 key	[SenderGIIN]_Payload
4	Encrypt AES key with public key of each recipient and For Model 1, Option 2 (only). Encrypt AES key with public key of HCTA	[ReceiverGIIN]_Key [HCTAGIIN]_Key
5	Create sender metadata	[SenderGIIN]_Metadata.xml
6	Create the transmission file	[UTC]_[SenderGIIN].zip
7	Transmit the package to IDES and receive delivery confirmation	N/A

Table 7 - Prepare and Transmit an XML File describes the process to prepare and send a file.

DRAFT

Step 1 - Prepare and Validate the FATCA XML File

Step 1 explains how to create a sender payload file. Each FATCA XML file contains information about the accounts required to be reported under FATCA. For information on the FATCA XML and related Form 8966 (FATCA Report), see FATCA XML Schemas and Business Rules for Form 8966.

Step 1a - Sign the XML File

Digital signatures provide the advantage of nonrepudiation and data integrity. Integrity ensures that the messages are not altered in transit. The receiver can verify that the received message is identical to the sent message. Nonrepudiation allows the sender of a message to be uniquely identified. A sender uses its own private key to digitally sign the message. Senders and recipients of FATCA files will be able to ensure that (1) the file was sent by a FATCA partner and (2) the file was not corrupted during compression, encryption, and decryption or altered during transmission to or from IDES.

Sign XML File:

Process	Descriptions	File Naming Convention
Sign XML File	▪ After validating the schema, digitally sign the FATCA XML file using W3C Recommendation XML Signature Syntax and Processing (Second Edition) "*Enveloping*" signature. ▪ To generate the digital signature[1], the XML file is processed by a "one-way hashing" algorithm to generate a fixed length message digest. ▪ IRS requires SHA2-256[2] hash with a 2048-bit RSA key as the standard for digitally signing FATCA files.	N/A
Summary	▪ The "*Enveloping*" digital signature is contained inside the "[SenderGIIN] _Payload.xml" file.	▪ [SenderGIIN]_Payload.xml

Table 8

[1] Digital Signature Standard (DSS) (FIPS 186-4), July 2013, nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[2] Secure Hash Standard (SHS) (FIPS 180-4), March 2012, csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

Step 2 - Compress the XML File

The XML file "[SenderGIIN]_Payload.xml" should be compressed using a compatible compression utility and the standard Deflate compression method.

Tools	Version	Host System
WinZip	17.5	Windows
7-Zip	9.2	Windows or Linux
Windows built-in zip utility	N/A	Windows
Linux/Unix standard zip utility	N/A	Linux/Unix
Apple built-in archive utility	MAC OS X 10.3 and later	MAC

Table 9- Recommended Compression Tools based on compression testing and supported algorithms.

DRAFT

Compress XML File:

Process	Descriptions	File Naming Convention
Compress XML File	▪ The compressed file "zip" is the file extension used by the compression tool or library ▪ Other tools may be used but the compression method must be recognized by one of the five tools or libraries for the file to be successfully processed	▪ [SenderGIIN]_Payload.zip
Summary	▪ If the file is not recognized or processing fails, the file will be rejected. The sending partner will receive a notification that explains the reason for the failure and how to modify and resubmit the file ▪ Note: The current supported compression is ZIP compression using the standard Deflate compression method	N/A

Table 10

Step 3 - Encrypt the XML File with AES 256 Key

AES is one of the most secure encryption algorithms and the preferred encryption standard for IDES. The file is encrypted to protect the FI and taxpayer sensitive information.

Encrypt XML File with AES Key:

Process	Descriptions	File Naming Convention
Encrypt XML File	▪ After compression, encrypt the file "[SenderGIIN]_ Payload.zip" using the AES-256 cipher with a randomly generated "one-time use" AES key. ▪ The AES encrypted file is called SenderGIIN]_Payload"	▪ [SenderGIIN]_Payload

Table 11

Additional information regarding the AES-256 encryption algorithm and keys can be found in:

- NIST Special Publication 800-57:
  Recommendation for Key Management – Part 1: General (Revision 3)
  csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
- Advanced Encryption Standard (FIPS 197), November 2001,
  csrc.nist.gov/publications/fips/fips197/fips-197.pdf

DRAFT

Step 4 - Encrypt the AES Key with Public Key of Recipient

The next step is to encrypt the AES key with the public key of each recipient. The file is encrypted to protect the AES key. All FATCA partners must validate the recipient's X.509 Digital Certificate to an approved CA. An X.509 Digital Certificate contains the public key for each FATCA partner, including the IRS, and is retrieved from the IDES Enrollment site.

Encrypt AES Key with Public Key:

Process	Descriptions	File Naming Convention
Validate Certificate	▪ To validate certificate: 1. Verify the certificate chain; 2. Check the revocation status of the certificate chain. There are two methods: ▪ Retrieve a Certificate Revocation List (CRL) or ▪ Send an Online Certificate Status Protocol (OCSP) query to a CA designated responder	N/A

Encrypt the AES Key	▪ After validating the certificate, use the public key from the recipient's certificate to encrypt the AES 256 key and specify "*PKCS7 with Padding*" ▪ The encrypted file is called "[ReceiverGIIN]_Key" "ReceiverGIIN" is the GIIN of the recipient of this AES key	▪ [ReceiverGIIN]_Key
Summary	▪ FATCA reporting with one recipient will have two encrypted files: 1. Symmetric encryption - the AES 256 encrypted FATCA XML file called "[SenderGIIN]_Payload" 2. Asymmetric encryption - the public key encrypted AES 256 key file called "[ReceiverGIIN]_Key"	N/A

Table 12

Note: For most FATCA partners (e.g., Model 1 (Non-Reciprocal), Model 2 and non-IGA) the IRS is the only recipient.

Step 5 - Encrypt the AES Key – Model 1, Option 2

Under IGA, Model 1, Option 2, an FI submits a FATCA XML file to IDES. The HCTA reviews and releases or denies the file to the IRS. The HCTA and the IRS will decrypt the same FATCA XML file. The FI creates a duplicate of the original AES 256 key. The duplicate AES 256 key is encrypted with the HCTA Public Key.

Encrypt AES Key – Model 1, Option 1:

Process	Descriptions	File Naming Convention
Validate Certificate	▪ See Step 4 – Validate Certificate	
Encrypt the AES Key	▪ After validating the certificate, use the public key from the recipient's certificate to encrypt the AES 256 key and specify "*PKCS7 with Padding*" ▪ The encrypted file is called "[ReceiverGIIN]_Key" "ReceiverGIIN" is the GIIN of the recipient of this AES key	▪ [ReceiverGIIN]_Key
Encrypt the AES Key	▪ Encrypt the AES key with the public key of the approving HCTA ▪ The encrypted file is called "[HCTAGIIN]_Key", where "HCTAGIIN" is the GIIN of the HCTA recipient of this AES key	▪ [HCTAGIIN]_Key
Summary	▪ FATCA reporting with two recipients should have three encrypted files: 1. Symmetric encryption - the AES 256 encrypted FATCA XML file called "[SenderGIIN]_Payload" 2. Asymmetric encryption - the public key encrypted AES 256 key file called "[ReceiverGIIN]_Key" 3. Asymmetric encryption - the public key encrypted AES 256 key file called "[HCTAGIIN]_Key"	N/A

Table 13

DRAFT

Step 6 - Create Sender Metadata File

Users can create a sender metadata file to ensure that recipients accurately process FATCA XML files and notifications. Notifications are responses sent by the IRS to an FI or HCTA and state whether the file was processed correctly or contained errors.

A template metadata file is available in XML format as part of the enrollment process. FIs and HCTAs can use the template to create a metadata file to attach to the payload before uploading to IDES.

The FATCA Sender Metadata XML file is created using the FATCA Metadata XML Schema v1.0 and the file will be called "[SenderGIIN]_Metadata.xml." All FATCA partners must provide the values for the elements in the sender metadata file. Refer to the FATCA XML Schemas page for more information.

Elements	Length	Description
FATCAEntitySenderId	N/A	FATCA partner that submits data
FATCAEntityReceiverId	N/A	FATCA partner receives data
FATCAEntCommunicationTypeCd	N/A	Indicates the transmission type RPT = FATCA reporting communication NTF = FATCA Notification communication
SenderFileId	200	References the user provided transmission filename
FileCreateTs	N/A	References timestamp created by the sender transmission
TaxYear	4	Indicates the tax year (YYYY format)
FileRevisionInd	1	Indicates if this is a revised transmission
OriginalIDESTransmissionId	32	IDES Transmission ID referencing an update to an earlier transmission Optional – Use only after IRS request
Optional – Use only after RCTA request	N/A	Optional - User email address

Table 14 - Sender Metadata Schema v1.0 lists and describes metadata schema elements.

Note: The sender metadata file is never encrypted because it is used to verify and route transmissions to the correct recipient.

Step 7 - Create a FATCA Data Packet

A file that is transmitted through IDES is known as a *FATCA data packet* or *data packet*. The data packet is an archive in

.ZIP file format, and it should be created using one of the compatible data compression tools described in Table 9. IDES only supports data packets in a .ZIP file format with a .zip file extension.

Model 1, Option 2	All Others
▪ [SenderGIIN]_Metadata.xml	▪ [SenderGIIN]_Metadata.xml
▪ [ReceiverGIIN]_Key	▪ [ReceiverGIIN]_Key
▪ [HCTAGIIN]_Key	▪ [SenderGIIN]_Payload
▪ [SenderGIIN]_Payload	

Table 15 – Transmission Summary lists files contained in a transmission archive or data packet.

The file naming convention of data packet is composed of a Coordinated Universal Time (UTC) timestamp and the GIIN of the sender (SenderGIIN) as:

[UTC]_[SenderGIIN].zip

The timestamp format of the UTC is YYYYMMDDTHHMMSSmsZ where:

YYYY = 4-digit year
MM = 2-digit month
DD = 2-digit day
HH = 24-hour
MM = 2-digit minutes
SS = 2-digit seconds
ms = 3-digit milliseconds

For example, a sender of GIIN “000000.00000.TA.ISO” that transmits a data packet on January 15, 2015 at 16:30:45 can create a data packet named as:

20150115T163045123Z_000000.00000.TA.ISO.zip

DRAFT

Step 8 - Transmit Data Packet using IDES

After the archive is uploaded and transmitted, IDES sends an alert to the authorized user via email. The message provides status information about the file upload. If the upload and IDES file checks are successful, IDES assigns a unique “TransmissionID” in the email. If there is an error, the IDES alert provides an appropriate error code in the email message.

Receiving a Notification Message from IRS

A notification is a transmission archive or data packet that contains encrypted documents sent from the IRS to an FI or HCTA. When the IRS sends a notification, IDES sends an email to the authorized user stating that a file is ready for download. The email correspondence includes the file name of the “TransmissionID” in the original file. Notifications are prepared using the same process and file components used to prepare the FATCA XML.

Users will need to download and unzip the notification message archive. IDES assigns each notification message a file name similar to the FATCA data report, such as [UTC]_[SenderGIIN].zip. Users can also process the elements contained in the IRS notification.

Note: In a Notification Message, the [SenderGIIN] is the IRS and [ReceiverGIIN] is either the HCTA or FI.

Steps	Process	File Naming Convention
1.	Validate the sender metadata file using the IRS Sender Metadata schema.	[SenderGIIN]_Metadata.xml
2.	Use your private key to decrypt the [ReceiverGIIN]_Key file	[ReceiverGIIN]_Key [HCTAGIIN]_Key
3.	Use the revealed AES key to decrypt the [SenderGIIN]_Payload.	[SenderGIIN]_Payload
4.	Decompress the [SenderGIIN]_Payload.zip	[SenderGIIN]_Payload.zip [SenderGIIN]_Payload.xml
5.	Validate “Enveloping” Digital Signature of the Notification XML file (the Payload).	N/A
6.	Validate the Notification XML file using the IRS notification schema.	N/A

Table 16- Notification Archive Summary describes how to open the archive.

DRAFT

Appendix A: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CRL	Certificate Revocation List
FATCA	Foreign Account Tax Compliance Act
FCPA	Federal Common Policy Root CA
FFI	Foreign Financial Institution
FI	Financial Institution
FTP	File Transfer Protocol
GIIN	Global Intermediary Identification Number
HCTA	Host Country Tax Authority
HTTPS	Hypertext Transfer Protocol Secure
IDES	International Data Exchange Service
IGA	Intergovernmental Agreement
IRS	Internal Revenue Service
NFFE	Non-Financial Foreign Entity
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PMO	Project Management Office
RSA	Rivest, Shamir and Adleman
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
TIEA	Tax Information Exchange Agreement
TLS	Transport Layer Security
UTC	Coordinated Universal Time

DRAFT

XML	Extensible Markup Language

Appendix B: File Naming Convention

File Name	Description	Associated IGA Group
[Sender]GIIN_Payload	Encrypted payload using a randomly generated one-time use key (preference: AES-256)	All
[Receiver]GIIN_Key	Key encrypted using the receiver public key	All
[Sender]GIIN_Metadata.xml	FATCA Metadata to ensure that recipients properly process FATCA XML reports. FATCA Metadata XSD will be published on the IRS website Note: A text version of the FATCA metadata [Sender]GIIN_Metadata.txt will be accepted for partners not familiar with xml.	N/A
[HCTA]GIIN_Key	Key encrypted using HCTA public key	Model1 Option 2
UTC_[SenderGIIN].zip	N/A	N/A

Note: N/A fields may be updated in final version of guide.

DRAFT

Appendix C: Certificate Upload Error Messages

Status	Description
CtlNotSignatureValid	Specifies that the certificate trust list (CTL) contains an invalid signature.
CtlNotTimeValid	Specifies that the certificate trust list (CTL) is not valid because of an invalid time value, such as one that indicates that the CTL has expired.
CtlNotValidForUsage	Specifies that the certificate trust list (CTL) is not valid for this use.
Cyclic	Specifies that the X509 chain could not be built.
HasExcludedNameConstraint	Specifies that the X509 chain is invalid because a certificate has excluded a name constraint.
HasNotDefinedNameConstraint	Specifies that the certificate has an undefined name constraint.
HasNotPermittedNameConstraint	Specifies that the certificate has an impermissible name constraint.
HasNotSupportedNameConstraint	Specifies that the certificate does not have a supported name constraint or has a name constraint that is unsupported.
InvalidBasicConstraints	Specifies that the X509 chain is invalid due to invalid basic constraints.
InvalidExtension	Specifies that the X509 chain is invalid due to an invalid extension.
InvalidNameConstraints	Specifies that the X509 chain is invalid due to invalid name constraints.
InvalidPolicyConstraints	Specifies that the X509 chain is invalid due to invalid policy constraints.
NoError	Specifies that the X509 chain has no errors.
NoIssuanceChainPolicy	Specifies that there is no certificate policy extension in the certificate. This error would occur if a group policy has specified that all certificates must have a certificate policy.
NotSignatureValid	Specifies that the X509 chain is invalid due to an invalid certificate signature.
NotTimeNested	Deprecated. Specifies that the CA (certificate authority) certificate and the issued certificate have validity periods that are not nested. For example, the CA cert can be valid from January 1 to December 1 and the issued certificate from January 2 to December 2, which would mean the validity periods are

DRAFT

	not nested.
NotTimeValid	Specifies that the X509 chain is not valid due to an invalid time value, such as a value that indicates an expired certificate.
NotValidForUsage	Specifies that the key usage is not valid.
OfflineRevocation	Specifies that the online certificate revocation list (CRL) the X509 chain relies on is currently offline.
PartialChain	Specifies that the X509 chain could not be built up to the root certificate.
RevocationStatusUnknown	Specifies that it is not possible to determine whether the certificate has been revoked. This can be due to the certificate revocation list (CRL) being offline or unavailable.
Revoked	Specifies that the X509 chain is invalid due to a revoked certificate.
UntrustedRoot	Specifies that the X509 chain is invalid due to an untrusted root certificate.

.

DRAFT